THE LONG FUSE:

MISINFORMATION AND THE 2020 ELECTION

ELECTION INTEGRITY PARTNERSHIP

The Long Fuse

Misinformation and the 2020 Election

The Election Integrity Partnership

Digital Forensic Research Lab
Graphika
Stanford Internet Observatory
UW Center for an Informed Public

2021

Identifiers: ISBN 978-1-7367627-1-4 (ebook)

1.3.0 (June 15, 2021)

Cover Illustration and Design by Alexander Atkins Design, Inc.

How to cite this work:

APA Style:

> Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory (2021). *The Long Fuse: Misinformation and the 2020 Election.* Stanford Digital Repository: Election Integrity Partnership. v1.3.0
> https://purl.stanford.edu/tr171zs0069

Chicago Style:

> Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory. *The Long Fuse: Misinformation and the 2020 Election*, 2021. Stanford Digital Repository: Election Integrity Partnership. v1.3.0
> https://purl.stanford.edu/tr171zs0069

Contents

Executive Summary

On January 6, 2021, an armed mob stormed the US Capitol to prevent the certification of what they claimed was a "fraudulent election." Many Americans were shocked, but they needn't have been. The January 6 insurrection was the culmination of months of online mis- and disinformation directed toward eroding American faith in the 2020 election.

US elections are decentralized: almost 10,000 state and local election offices are primarily responsible for the operation of elections. Dozens of federal agencies support this effort, including the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security, the United States Election Assistance Commission (EAC), the FBI, the Department of Justice, and the Department of Defense. However, none of these federal agencies has a focus on, or authority regarding, election misinformation originating from domestic sources within the United States. This limited federal role reveals a critical gap for non-governmental entities to fill. Increasingly pervasive mis- and disinformation, both foreign and domestic, creates an urgent need for collaboration across government, civil society, media, and social media platforms.

The Election Integrity Partnership, comprising organizations that specialize in understanding those information dynamics, aimed to create a model for whole-of-society collaboration and facilitate cooperation among partners dedicated to a free and fair election. With the narrow aim of defending the 2020 election against voting-related mis- and disinformation, it bridged the gap between government and civil society, helped to strengthen platform standards for combating election-related misinformation, and shared its findings with its stakeholders, media, and the American public. This report details our process and findings, and provides recommendations for future actions.

Who We Are: EIP and Its Members

The Election Integrity Partnership was formed to enable real-time information exchange between election officials, government agencies, civil society organizations, social media platforms, the media, and the research community.[1] It aimed to identify and analyze online mis- and disinformation, and to communicate important findings across stakeholders. It represented a novel collaboration between four of the nation's leading institutions focused on researching mis- and disinformation in the social media landscape:

- The Stanford Internet Observatory (SIO)
- The University of Washington's Center for an Informed Public (CIP)
- Graphika
- The Atlantic Council's Digital Forensic Research Lab (DFRLab)

What We Did

The EIP's primary goals were to: (1) identify mis- and disinformation before it went viral and during viral outbreaks, (2) share clear and accurate counter-messaging, and (3) document the specific misinformation actors, transmission pathways, narrative evolutions, and information infrastructures that enabled these narratives to propagate. To identify the scope of our work, we built a framework to compare the policies of 15 social media platforms[2] across four categories:

- *Procedural interference*: misinformation related to actual election procedures
- *Participation interference*: content that includes intimidation to personal safety or deterrence to participation in the election process
- *Fraud*: content that encourages people to misrepresent themselves to affect the electoral process or illegally cast or destroy ballots
- *Delegitimization of election results*: content aiming to delegitimize election results on the basis of false or misleading claims

The EIP used an innovative internal research structure that leveraged the capabilities of the partner organizations through a tiered analysis model based on "tickets" collected internally and from our external stakeholders. Of the tickets we processed, 72% were related to delegitimization of the election.

Key Takeaways

Misleading and false claims and narratives coalesced into the meta-narrative of a "stolen election," which later propelled the January 6 insurrection.

- Right-leaning "blue-check" influencers transformed one-off stories, sometimes based on honest voter concerns or genuine misunderstandings, into cohesive narratives of systemic election fraud.
- Warped stories frequently centered on mail-in voting and accusations of found, discarded, or destroyed ballots, particularly in swing states. Misleading framing of real-world incidents often took the form of falsely assigning intent, exaggerating impact, falsely framing the date, or altering locale.
- The meta-narrative of a "stolen election" coalesced into the #StopTheSteal movement, encompassing many of the previous narratives. The narrative appeared across platforms and quickly inspired online organizing and offline protests, leading ultimately to the January 6 rally at the White House and the insurrection at the Capitol.
- Fact-checking of narratives had mixed results; non-falsifiable narratives presented a particular challenge. In some cases, social media platform fact-checks risked drawing further attention to the claims they sought to debunk.

The production and spread of misinformation was multidirectional and participatory.

- Individuals participated in the creation and spread of narratives. Bottom-up false and misleading narratives started with individuals identifying real-world or one-off incidents and posting them to social media. Influencers and hyperpartisan media leveraged this grassroots content, assembling it into overarching narratives about fraud, and disseminating it across platforms to their large audiences. Mass media often picked up these stories after they had reached a critical mass of engagement.
- Top-down mis- and disinformation moved in the opposite direction, with claims first made by prominent political operatives and influencers, often on mass media, which were then discussed and shared by people across social media properties.

Narrative spread was cross-platform: repeat spreaders leveraged the specific features of each platform for maximum amplification.

- The cross-platform nature of misinformation content and narrative spread limited the efficacy of any single platform's response.
- Smaller, niche, and hyperpartisan platforms, which were often less moderated or completely unmoderated, hosted and discussed content that had been moderated elsewhere. Parler in particular saw a remarkable increase in its active user base, as users rejected the "censorship" they perceived on other platforms.

The primary repeat spreaders of false and misleading narratives were verified, blue-check accounts belonging to partisan media outlets, social media influencers, and political figures, including President Trump and his family.

- These repeat spreaders amplified the majority of the investigated incidents aggressively across multiple platforms.
- Repeat spreaders often promoted and spread each others' content. Once content from misleading narratives entered this network, it spread quickly across the overlapping audiences.

Many platforms expanded their election-related policies during the 2020 election cycle. However, application of moderation policies was inconsistent or unclear.

- Platforms took action against policy violations by suspending users or removing content, downranking or preventing content sharing, and applying informational labels. However, moderation efforts were applied inconsistently on and across platforms, and policy language and updates were often unclear.
- Account suspensions and content removal or labeling sometimes contributed to conspiratorial narratives that platforms were "covering up the truth," entangling platforms with the narratives they wished to eliminate.
- Lack of transparency and access to platform APIs hindered external research into the effectiveness of platform policies and interventions.

Key Recommendations

Federal Government

- Establish clear authorities and roles for identifying and countering election related mis- and disinformation. Build on the federal interagency movement toward recognizing elections as a national security priority and critical infrastructure.
- Create clear standards for consistent disclosures of mis- and disinformation from foreign and domestic sources as a core function of facilitating free and fair elections, including via CISA's Rumor Control and joint interagency statements.

Congress

- Pass existing bipartisan proposals for increased appropriations marked for federal and state election security.
- Codify the Senate Select Committee on Intelligence's bipartisan recommendations related to the depoliticization of election security and the behavior of public officials and candidates for federal office noted in Volumes 3 and 5 of the Committee's report on foreign influence in 2016 elections.

State and Local Officials

- Establish trusted channels of communication with voters. This should include a .gov website and use of both traditional and social media.
- Ensure that all votes cast are on auditable paper records and that efficient, effective, and transparent post-election audits are conducted after each election.

Platforms

- Provide proactive information regarding anticipated election misinformation. For example, if researchers expect a narrative will emerge, platforms should explain that narrative's history or provide fact-checks or context related to its prior iterations.
- Invest in research into the efficacy of internal policy interventions (such as labeling) and share those results with external researchers, civil society, and the public.

- Increase the amount and granularity of data regarding interventions, take-downs, and labeling to allow for independent analysis of the efficacy of these policies.
- Impose clear consequences for accounts that repeatedly violate platform policies. These accounts could be placed on explicit probationary status, facing a mixture of monitoring and sanctions.
- Prioritize election officials' efforts to educate voters within their jurisdiction and respond to misinformation. This could include the promotion of content from election officials through curation or advertisement credits, especially in the lead-up to Election Day.

Conclusion

The 2020 election demonstrated that actors—both foreign and domestic—remain committed to weaponizing viral false and misleading narratives to undermine confidence in the US electoral system and erode Americans' faith in our democracy. Mis- and disinformation were pervasive throughout the campaign, the election, and its aftermath, spreading across all social platforms. The Election Integrity Partnership was formed out of a recognition that the vulnerabilities in the current information environment require urgent collective action.

While the Partnership was intended to meet an immediate need, the conditions that necessitated its creation have not abated, and in fact may have worsened. Academia, platforms, civil society, and all levels of government must be committed, in their own ways, to truth in the service of a free and open society. All stakeholders must focus on predicting and pre-bunking false narratives, detecting mis- and disinformation as it occurs, and countering it whenever appropriate.

Notes

1. (page vi) "Announcing the EIP," Election Integrity Partnership, July 27, 2020, https://www.eipartnership.net/news/announcing-the-eip

2. (page vi) The platforms evaluated during EIP's operation include: Facebook, Instagram, Twitter, YouTube, Pinterest, Nextdoor, TikTok, Snapchat, Parler, Gab, Discord, WhatsApp, Telegram, Reddit, and Twitch. Twitch was added to our list during our blog post update in October.

Contributors

The EIP was supported by the following students, staff and researchers from the four partner organizations.

Stanford Internet Observatory
Samantha Bradshaw
Daniel Bush
Jack Cable
Caleb Chiam
Elena Cryst
Matt DeButts
Renée DiResta
Emma Dolan
Ayelet Drazen
Jackson Eilers
Ross Ewald
Toni Friedman
Isabella García-Camargo
Josh Goldstein
Shelby Grossman
Sejal Jhawer
Jennifer John
Katie Jonsson
Dylan Junkin
Ananya Karthik
Tara Kheradpir
Soojong Kim
Nazli Koyluoglu
Kevin Lin
Pierce Lowary
Sahar Markovich
Gordon Martinez-Piedra
Miles McCain
Malika Mehrotra
Carly Miller
Nandita Naik
Benjamin Newman
Ana Sofia Nicholls
Shelby Perkins
Ashwin Ramaswami
Cooper Raterink
Cooper Reed
Emily Ross
Abuzar Royesh
Danny Schwartz
Chase Small
Alex Stamos
Gene Tanaka
David Thiel
Julia Thompson
Yesenia Ulloa
Alessandro Vecchiato
Netta Wang
Lyndsea Warkenthien
Alex Zaheer

UW Center for an Informed Public
Joseph Bak-Coleman
Andrew Beers
Nicole Buckley
Michael Caufield (WSU)
Michael Grass
Melinda McClure Haughey
Ian Kennedy
Kolina Koltai
Paul Lockaby
Rachel Moran
Joey Schafer
Emma Spiro
Kate Starbird
Morgan Wack
Jevin West
Tom Wilson
Martin Zhang

Graphika
Joseph Carter
Avneesh Chandra
Shawn Eib
Rodrigo Ferreira
Camille François
Thomas Lederer
Erin McAweeney
Vanessa Molter
Morgan Moon
Jack Nassetta
Ben Nimmo
Brian Potochney
Léa Ronzaud
Melanie Smith
Kyle Weiss

DFRLab
Eric Baker
Graham Brookie
Emerson Brooking
Kelsey Henquinet
Alyssa Kann
Ayushman Kaul
Zarine Kharazian
Tessa Knight
Jean le Roux
Jacqueline Malaret
Esteban Ponce de Leon
Max Rizzuto
Iain Robertson
Michael Sheldon
Helen Simpson

This report was edited by Eden Beck and designed by David Thiel. The Election Integrity Partnership would like to thank Matthew Masterson for additional feedback, and Nate Persily for his support.

Acknowledgements

The Election Integrity Partnership's partners wish to acknowledge the following organizations for the generous financial support through which this report was possible:

Digital Forensic Research Lab, The Atlantic Council

The Digital Forensic Research Lab is part of and funded by the Atlantic Council. A full list of the Atlantic Council's donors is available at:

https://www.atlanticcouncil.org/in-depth-research-reports/report/annual-report-2019-2020-shaping-the-global-future-together/

Graphika

Graphika thanks the Omidyar Network for their support on this project.

Stanford Internet Observatory

The Stanford Internet Observatory thanks its operational funders, Craig Newmark Philanthropies and the William and Flora Hewlett Foundation, for their ongoing support.

University of Washington Center for an Informed Public

The Center for an Informed Public (CIP) thanks Craig Newmark Philanthropies and the Omidyar Network for their support of this project. Additional operational and research support for the CIP is provided by the John S. and James L. Knight Foundation and the William and Flora Hewlett Foundation. Researchers who contributed to the EIP also receive partial support from the U.S. National Science Foundation (grants 1749815 and 1616720), the Eunice Kennedy Shriver National

Institute of Child Health and Human Development (training grant T32 HD101442-01 to the Center for Studies in Demography & Ecology at the University of Washington), the University of Washington UW Population Health Initiative, and Microsoft. A full list of CIP donors is available at: https://www.cip.uw.edu/about/

Chapter 1

The Election Integrity Partnership

1.1 Introduction

The 2016 presidential election in the United States demonstrated to the world the potential of wide-scale information operations. Since 2016, these efforts have grown, often aimed at developed democracies and operated by state-sponsored adversaries and domestic activists alike. Misinformation and disinformation can disenfranchise voters and diminish trust in the results of electoral contests, eroding public confidence in the integrity of democratic processes and leadership transitions overall. For the purposes of this report, we use "misinformation" as an umbrella term to describe false, misleading, or exaggerated information or claims. We differentiate this from "disinformation," which is false or misleading information that is *purposefully* produced, seeded, or spread, with the intent to manipulate in service to an objective; the manipulation may also take the form of leveraging fake accounts or pages. (We define these terms more fully in Appendix A on page 245: Definitions).

Elections in the United States are highly decentralized.[1] Over 10,000 individual jurisdictions—covering state, county, and municipal levels—are responsible for administering the vote on Election Day. Voter registration systems and databases are centralized at the state level in some states and administered by states, counties, and municipalities in others. Vote casting, in contrast, is organized at the local level, with each locality responsible for administering ballots, counting votes, and educating voters about the local system.[2] There is no centralized support to aid this vast number of jurisdictions in identifying and responding to emerging election-related mis- and disinformation.

In 2020, adding to the complexity, the global COVID-19 pandemic forced rapid changes to voting procedures. States and counties had to quickly adapt their electoral processes to new public health guidelines. Existing state laws on elec-

tion procedure were in many cases not adaptable to the emergency conditions, leading to late executive and legislative action and court decisions.[3]

Voters, many of whom were sheltering at home, followed election conversations on broadcast as well as social media. This included searching for information about where and how to vote in light of pandemic restrictions.

The initial idea for the Partnership came from four students that the Stanford Internet Observatory (SIO) funded to complete volunteer internships at the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security. Responsibility for election information security is divided across government offices: CISA has authority to coordinate on cybersecurity issues related to the election, the FBI to investigate cyber incidents and enforce election laws, and intelligence agencies to monitor for foreign interference. Yet, no government agency in the United States has the explicit mandate to monitor and correct election mis- and disinformation. This is especially true for election disinformation that originates from within the United States, which would likely be excluded from law enforcement action under the First Amendment and not appropriate for study by intelligence agencies restricted from operating inside the United States. As a result, during the 2020 election, local and state election officials, who had a strong partner on election-system and overall cybersecurity efforts in CISA, were without a clearinghouse for assessing mis- and disinformation targeting their voting operations. The students approached SIO leadership in the early summer, and, in consultation with CISA and other stakeholders, a coalition was assembled with like-minded partner institutions.

The Election Integrity Partnership (EIP) was officially formed on July 26, 2020—100 days before the November election—as a coalition of research entities who would focus on supporting real-time information exchange between the research community, election officials, government agencies, civil society organizations, and social media platforms.

1.2 The EIP: Partner Organizations and Structure

The Partnership was formed between four of the nation's leading institutions focused on understanding misinformation and disinformation in the social media landscape: the Stanford Internet Observatory, the University of Washington's Center for an Informed Public, Graphika, and the Atlantic Council's Digital Forensic Research Lab.

The **Stanford Internet Observatory** (SIO) was founded in June 2019 to study the misuse of the internet to cause harm, formulate technical and policy responses to said misuse, and teach the next generation how to avoid the mistakes of the past. Founded by former Silicon Valley cybersecurity executive Alex Stamos, the

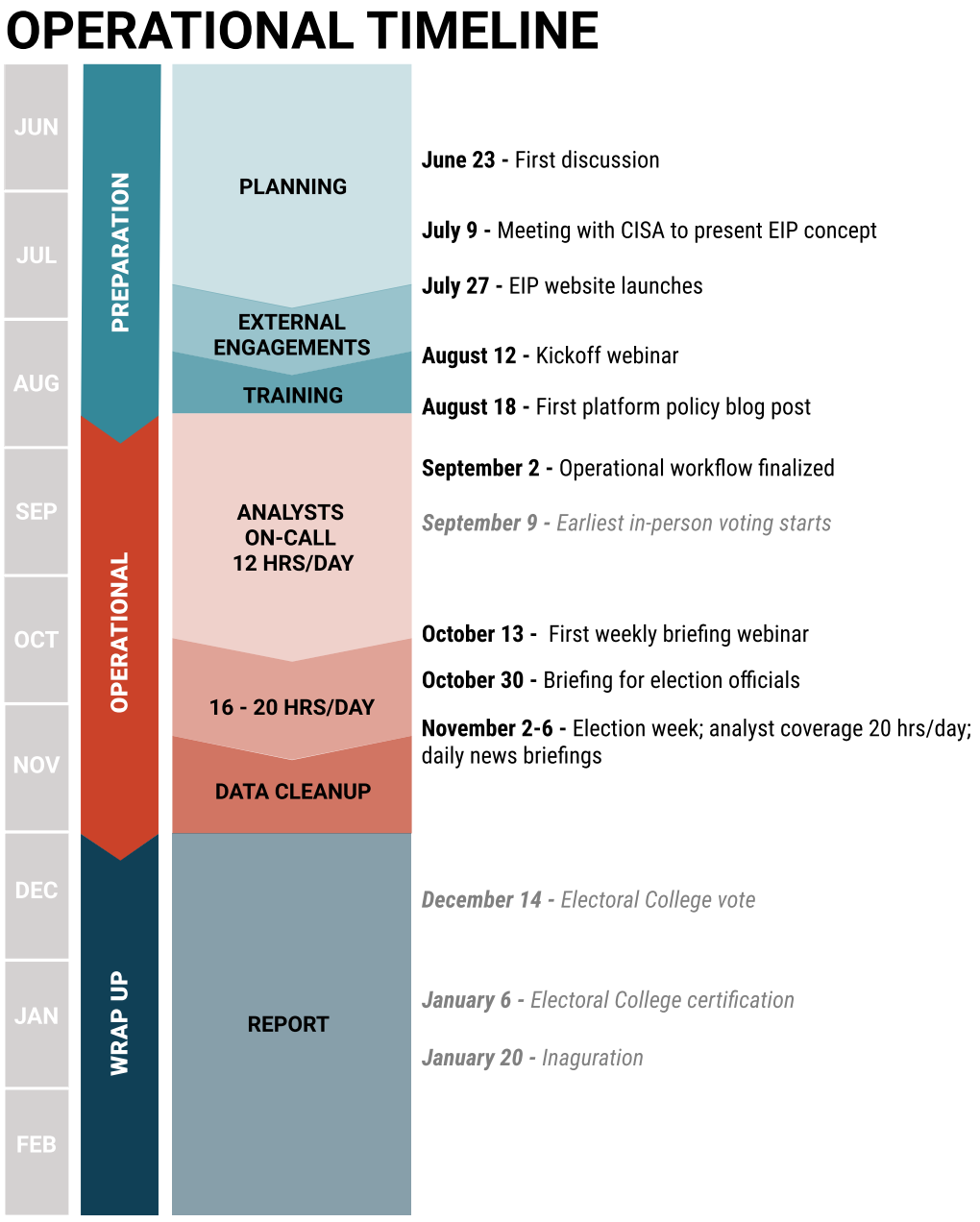

Figure 1.1: Timeline of the Election Integrity Partnership's work.

Observatory has a specific interest in applying the learnings of major technology platforms from the 2016 election to prevent a repeat in future years. The Observatory sits at Stanford's Cyber Policy Center under the direction of Professors Nate Persily and Dan Boneh.

The Internet Observatory team was led by Assistant Director Elena Cryst, Research Manager Renée DiResta, CTO David Thiel, and Director Alex Stamos. SIO graduate student Isabella García-Camargo served as the project manager for the overall Partnership. SIO engaged its team of seven staff researchers and five postdoctoral scholars from the Stanford Cyber Policy Center, and hired a team of 38 undergraduate and graduate research assistants from Stanford to serve as analysts on the project.

The **University of Washington Center for an Informed Public** (CIP) was founded in December 2019 with the mission of marshalling the resources of a public university to address mis- and disinformation through research, education, policy development, and outreach. The Center's interdisciplinary faculty brought deep methodological expertise at systematically analyzing "big" social data at macro-, meso-, and micro- scales to track the spread of misinformation online, and contextual expertise in online disinformation.

The CIP contributing team was led by three founding faculty members: Kate Starbird, Emma Spiro, and Jevin West. The team also included one affiliate faculty member, three postdoctoral researchers (all of whom started after the Partnership launched), nine undergraduate and PhD students from the University of Washington, a data engineer, and a communications specialist.

Graphika is a social media analytics firm trusted by Fortune 500 companies, human rights organizations, and universities to map and navigate complex social media landscapes. The company was founded in 2013 by Dr. John Kelly, a pioneer in this field and source of expert testimony on foreign interference in the 2016 US presidential election before the Senate Select Committee on Intelligence. Graphika helps partners around the world to discover how communities form online and map the flow of influence and information within large-scale social networks. It reports on information operations carried out by various foreign actors around the world. In addition, Graphika regularly briefs the House and Senate Intelligence Committees on a range of topics, including the growth of the QAnon movement and the spread of misinformation around COVID-19.

Graphika's team was led by their Chief Innovation Officer Camille François and Head of Analysis Melanie Smith, and included 13 analysts, data scientists, and open source investigators. This unique combination of skills and expertise enables Graphika to take an innovative approach to detecting and monitoring disinformation.

The **Digital Forensic Research Lab** (DFRLab) was founded at the Atlantic Council

in 2016 to operationalize the study of disinformation by exposing falsehoods and fake news, documenting human rights abuses, and building digital resilience worldwide. Its mission is to identify, expose, and explain disinformation where and when it occurs using open source research, create a new model of expertise adapted for impact and real-world results, and forge digital resilience at a time when humans are more interconnected than at any point in history.

DFRLab's contributing team was led by Director Graham Brookie and Resident Fellow Emerson Brooking and included 13 DFRLab research assistants and communications staff. These professionals brought extensive digital forensic research experience and language skills to the work of the Partnership.

The EIP was not set up as a legal entity; rather, it was a consortium based on good-faith agreements. While future models should certainly consider more formal arrangements, the time-sensitive nature of the project required organizations to rely on interinstitutional trust and rapport built over several years of collaboration.

1.3 The EIP: Goals and Scope

The stated objective of the EIP was to detect and mitigate the impact of attempts to prevent or deter people from voting or to delegitimize election results.[4] The EIP was not a fact-checking partnership, and was not focused on debunking misinformation more generally; our objective explicitly excluded addressing comments made about candidates' character or actions and was focused narrowly on content intended to suppress voting, reduce participation, confuse voters as to election processes, or delegitimize election results without evidence (see Table 1.1 on the next page).

To determine what was in and out of scope for the EIP, one of our first tasks was to build a framework that identified potential types of election-related mis- and disinformation. This process identified four core categories that we defined as our scope of focus (see Table 1.2 on page 7).

GOALS OF THE ELECTION INTEGRITY PARTNERSHIP		
Goal 1: **Identify misinformation** before it goes viral.	Goal 2: Share clear, accurate **counter-messaging**.	Goal 3: Increase **transparency** into what happened during the 2020 elections.
Activities		
• Establish a collaboration between the top misinformation research organizations • Operationalize the misinformation research process with tiered research and workspace management systems • Train analysts to identify cross-platform trends for earlier platform notification and action when appropriate	• Build critical bridges between election officials, platforms, and civil society organizations • Provide local and state officials with a partner that could research and help mitigate misinformation about their local operations • Generate rapid research findings that have the ability to disrupt the misinformation environment in real time	• Collect data in real-time for empirical analysis that would be difficult to assemble after the fact • Build an annotated database of archived misinformation content • Provide visibility into how narratives spread across multiple social media platforms
Outputs		
• Flag policy violations to platforms • Communicate to stakeholders	• Live media briefings • Blog posts • Tweet threads	• Final report • Dataset of content for future academic use

Table 1.1: Goals of the Election Integrity Partnership.

SCOPE OF THE ELECTION INTEGRITY PARTNERSHIP			
Procedural Interference: Misleading or false information about the actual election procedures. Content directly related to dates and components of the voting process that prevents people from engaging in the electoral process.	**Participation Interference:** Content that deters people from voting or engaging in the electoral process, sometimes related to voter suppression or intimidation.	**Fraud:** Content that encourages people to misrepresent themselves to affect the electoral process or illegally cast or destroy ballots.	**Delegitimization of Election Results:** Content that delegitimizes election results on the basis of false or misleading claims.
Example Content			
Content that misleads voters about how to correctly sign a mail-in ballot. Content that encourages voters to vote on a different day.	Content that affects the desire or perceived safety of voters engaging in the electoral process. Misleading or false information about the length of lines at a polling station, to deter in-person voting.	Offers to buy or sell votes with cash or gifts. Calls for non-citizens to vote.	Claims of fraud or malfeasance with inaccurate or missing evidence.

Table 1.2: Scope of the Election Integrity Partnership.

In addition to determining the EIP's scope, this content-centric framework enabled us to evaluate and compare platform policies across 15 different popular social media platforms in the US, and to help civil society, government, academia, and the public better understand what election-related content platforms can and will moderate.[5]

Organizational Structure and Workflow Management

One of the innovative aspects of the EIP was its internal research structure, which had to operationalize the misinformation research process in such a way as to best leverage the capabilities of the partner organizations. There is often an abundance of data involved in the analysis of information operations, and the process of following threads can take weeks or months. In order to meet the need for real-time or rapid analysis while maintaining the high standard of investigations that each partner holds itself to, the Partnership developed a tiered analysis model that leveraged "on-call" staffing of different analyst types.

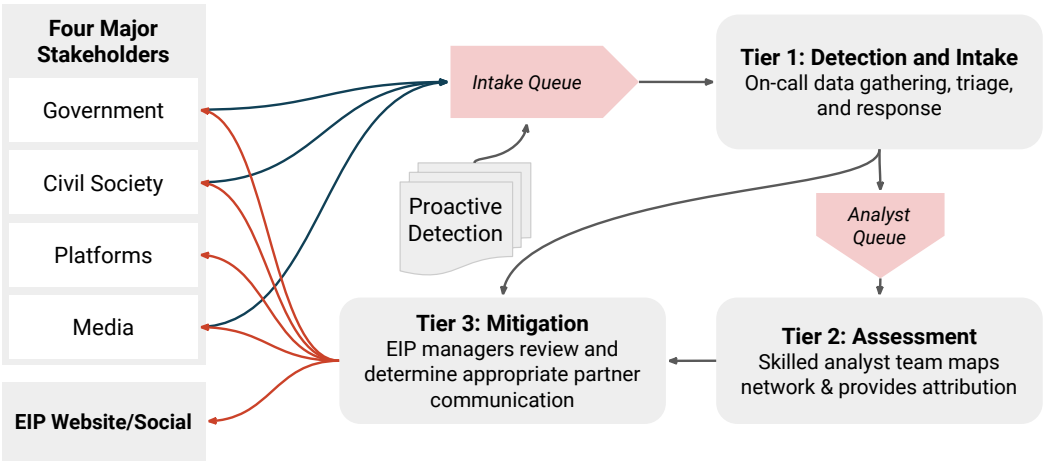

Figure 1.2: The EIP internal workflow. Filed tickets moved through the listed queues per the directional arrows.

The EIP tracked its analysis topics and engaged with outside stakeholder organizations using an internal ticketing workflow management system. Each identified informational event was filed as a unique ticket in the system.[6] Tickets were submitted by both trusted external stakeholders (detailed in Section 1.4 on page 11) and internal EIP analysts. For example, an email from an external stakeholder to the dedicated tip line would automatically generate a ticket to the internal team for quick response. Similarly, if during online monitoring an analyst came across a piece of content that might be an instance of election-related misinformation, that analyst would open a ticket on the case and put it

in the analyst queue for investigation. A single ticket could map to one piece of content, an idea or narrative, or hundreds of URLs pulled in a data dump. The ticket tracked analysts' research into this event, comments from platform partners, and other developments. Related tickets were then grouped into distinct information events or incidents, described more in Chapter 5.[7]

Analysis Tiers

Each ticket traveled through a series of analysis queues before reaching a final resolution. In the investigation process, analysts completed specific forms that contained a series of required fields detailing the information incident and documented essential data such as target audience, subject, engagement, and spread. The overall research process was broken down into three phases: detection, assessment, and mitigation.

- **Tier 1: Detection** — Tier 1 analysts were tasked with conducting the initial analysis on and archiving of potential incidents. These analysts also searched for potential in-scope content by tracking public social media posts to surface incidents. To ensure coverage in the monitoring process, each analyst was assigned to a specific state or interest group (see Section 3.3), which they developed expertise in and followed throughout the project. These analysts classified tickets as in and out of scope for further analysis and closed incidents for which further investigation or external communication was not needed. For in-scope tickets, analysts went through a systematic process that attempted—where possible—to assess the veracity of the underlying claims by locating an external fact-check from election officials, fact-checking organizations, local media, or mainstream outlets. They also made initial recommendations on the prioritization of tickets, assigning high, medium, and low severity based on the risk of the content itself and on its spread across platforms.[8]
- **Tier 2: Assessment** — This team was staffed by senior analysts from each partner organization. Analysts used open source intelligence and other social media analysis methods to delve deeper into the initial analysis from Tier 1 by determining the suspected origins of a piece of information, tracking its spread over time, and identifying additional fact-checks as they became available. Tier 2 analysts also looked for evidence of coordination, potential foreign interference, or inauthentic dynamics related to a given incident. This tier of analysts could recommend actions, such as communication to external partners, as appropriate.
- **Tier 3 (Managers): Mitigation** — This team consisted of leadership from each partnership organization, who signed off on the communication recommendations from Tier 2 senior analysts. The manager had the ability

to tag platform partners on a ticket for action. They also communicated with the EIP's partners in government, and could request further information from election officials if necessary. Once a ticket reached Tier 3, the manager decided whether to put it into a holding queue for ongoing monitoring, assign the ticket back to a Tier 2 analyst to produce a public blog post or Twitter thread discussing the issue, or close a ticket if it had been resolved.

Team members from each of these tiers were divided into on-call shifts. Each shift was four hours long and led by one on-call manager. It was staffed by a mix of Tier 1 and Tier 2 analysts in a 3:1 ratio, ranging from five to 20 people. Analysts were expected to complete between two to five shifts per week. The scheduled shifts ran from 8:00 am to 8:00 pm PT for most of the nine weeks of the partnership, ramping up only in the last week before the election from 12-hour to 16- to 20-hour days with all 120 analysts on deck.

A note on fact-checking: the EIP was not a fact-checking organization, and in preliminary assessments of whether an event in a ticket was potentially misinformation, analysts first looked to the work of others. One of the complexities related to misleading information is that it is not always possible to verify the claims; professional fact-checkers confronted with these situations may use labels like "inconclusive" or "partially true" to convey uncertainty where it exists. Where possible, our analysts identified an external fact-checking source from news sites, credible fact-checking organizations, or statements from a local election official when filing tickets. Analysts also used open source investigation techniques, such as reverse image searches or location identifications, to determine if images or videos tied to an incident were taken out of their original context. Our analysts identified at least one external fact-check source for approximately 42% of the in-scope tickets. For some tickets, it was not possible to find an external fact-check for the content, either because no fact-checker had yet addressed the issue, or because the information was resistant to simple verification—for example, content based on unconfirmed or conflicting claims from a whistleblower, conspiracy theories that claimed invisible forces at work, and narratives based on factual claims (e.g., discarded ballots) but spread within misleading frames that exaggerated the potential impact of these events. Additionally, some tickets were about incitement to violence, which does not lend itself to fact-checking.

Election Day-Specific Structures

In the week before and after Election Day, EIP monitoring intensified significantly. Over the two-month-long period from September 3 (the first day of EIP activity) to November 1, EIP researchers had logged 269 tickets. From November 2 to 4,

EIP researchers logged an additional 240 new tickets, as well as monitoring and revising old cases as they related to new narratives. This dramatic increase in tempo required changes to how the EIP identified and evaluated misinformation incidents.

In order to manage an anticipated increase in incidents on Election Day itself, the EIP established five working groups, each organized and led by relevant subject matter experts:

- *State and Regional Monitoring* focused on monitoring narratives related to polling locations in battleground states, particularly Pennsylvania, Wisconsin, Florida, and Minnesota. Analysts used platform search features coupled with curated CrowdTangle, Twitter, and Junkipedia lists to aid in detection.
- "*Targeted Group*" *Monitoring* focused on identifying misinformation that seemed to specifically target an ethnic or diaspora community in the United States. This included content targeting the Black community, which was the subject of extensive disinformation campaigns in 2016, as well as Chinese- and Spanish-language content.
- *Influencers and Young Electorate Monitoring* focused on first-time voters, particularly members of Generation Z. This work was conducted by way of close analysis of TikTok and Instagram trends.
- *Political Extremism Monitoring* focused on communities that had previously endorsed political violence, particularly those adjacent to White-identitarian causes. This work was conducted by comprehensive monitoring across 4chan, 8kun, Gab, and Parler. Researchers additionally monitored open Telegram channels and Discord servers linked to extremist causes.
- *Livestream Monitoring* focused on rapidly identifying trending livestreams, which were anticipated to involve both polling location activity and (later) election night protests. This work required assessing popular livestreams across Facebook Live, Periscope, YouTube Live, and Twitch.

These working groups would provide the foundation of EIP monitoring efforts in both the Election Day and post-Election Day periods.

1.4 External Stakeholders

The EIP served as a connector for many stakeholders, who both provided inputs to and received outputs from the internal analysis structure described

above. External stakeholders included government, civil society, social media companies, and news media entities.

Government and civil society partners could create tickets or send notes to EIP analysts, and they used these procedures to flag incidents or emerging narratives to be assessed by EIP analysts. Sometimes the tickets were out of scope, such as those related to general political misinformation that was not election related. In these cases, that was communicated to the reporting partner and the incident was closed. For all that were in scope, the EIP quickly analyzed the issues and provided outputs to external stakeholders. Some of the cases flagged by outside partners led to EIP participation in informing the public of a finding, which was done by way of a rapid-response blog post or Twitter thread, or a discussion during public media briefings.

Figure 1.3: Major stakeholder groups that collaborated with the EIP.

Government

Given the decentralized nature of election administration, government entities at the local, state, and federal level are all responsible in some way for election security and thus for countering election-related mis- and disinformation.

Prior to the 2016 election, the federal government played a very limited role in election security. Russian interference in the 2016 US presidential election took the form of several Russia-linked entities engaged in a broad interference effort that included information operations and targeting of election infrastructure as well as hack-and-leak attacks. Operatives of the Russia-based Internet Research Agency used social media to degrade Americans' confidence in their own

democratic process. Since 2016, the US government has declared election systems critical infrastructure and politicians have called for a "whole-of-society" approach to countering attacks against them.[9]

EI-ISAC: Coordination Across State And Local Government

After the 2016 election, government entities at all levels stepped up election security efforts; however, addressing election-related misinformation has remained a gap. For the 2020 election, reporting falsehoods about the election to social media platforms represented significant logistical and jurisdictional challenges. The Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), an independent organization run by the non-profit Center for Internet Security (CIS) that connects state and local governments as well as relevant private companies, helps coordinate election security efforts broadly. In this election cycle, the EI-ISAC served as a singular conduit for election officials to report false or misleading information to platforms. By serving as a one-stop reporting interface, the EI-ISAC allowed election officials to focus on detecting and countering election misinformation while CIS and its partners reported content to the proper social media platforms. Additionally, the Countering Foreign Influence Task Force (CFITF), a subcomponent of CISA, aided in the reporting process and in implementing resilience efforts to counter election misinformation.

The EIP engaged with government stakeholders primarily to provide analytical capability and context around election-related misinformation. Content reported by election officials to the EI-ISAC was also routed to the EIP ticketing system. This allowed analysts to find similar content, ascribe individual content pieces to broader narratives, and determine virality and cross-platform spread if applicable. This analysis was then passed back to election officials via the EI-ISAC for their situational awareness, as well as to inform potential counter-narratives. Additionally, if an internally generated EIP ticket targeted a particular region, analysts sent a short write-up to the EI-ISAC to share with the relevant election official. This allowed the state or local official to verify or refute the claim, and enabled analysts to properly assess whether or not the content violated a platform's civic integrity policies. In this way, the EIP demonstrated the upside of using the EI-ISAC coordinating body to connect platforms with authoritative voices to determine truth on the ground and help election officials effectively counter viral falsehoods about election infrastructure.

Civil Society

Civil society organizations fill critical roles in promoting civic engagement, and in organizing and sharing information with their communities. The EIP engaged

with civil society organizations to share findings and build perspective across geographies and demographics. Civil society collaborators submitted tips through the trusted partner tip line and interacted with the EIP research team through briefings, partner meetings, and shared findings. The Partnership engaged with Common Cause,[10] national and regional chapters of the NAACP,[11] the Healthy Elections Project,[12] the Defending Digital Democracy Project,[13] MITRE,[14] regional chapters of the AARP,[15] and the National Conference on Citizenship[16] (the latter two are discussed in more detail below). Some collaborators were integrated into the Jira platform for tip reporting, while others preferred to engage in a more informal capacity such as via email. Onboarded members were able to submit tickets for analysis and receive feedback from the EIP analysts.

The AARP collaboration was maintained by the Center for an Informed Public and was notable because it involved empowering and training retired adults to identify false or misleading information as part of a "Factcheck Ambassador" training program. The EIP worked primarily with the Washington State chapter of the AARP, but informational training sessions were shared with other chapters around the country.[17]

Another noteworthy civil society partner was the National Conference on Citizenship, specifically their Junkipedia team.[18] Junkipedia is a research tool created by the Algorithmic Transparency Institute, a project of the National Conference on Citizenship, to collect false and misleading social media content. The tool served dual purposes: first, it connected EIP to content surfaced through its own network of journalists and reporters, providing visibility into more geographies and communities; and second, it facilitated research and detection by EIP analysts, who were able to use Junkipedia's list feature to track account activity on TikTok and YouTube.

Media

Carefully considered media coverage debunking false and misleading information can help to ensure an informed public and a responsible social media ecosystem. Although mis- and disinformation monitoring and analysis work is valuable on its own, communications with media organizations increased the impact of the EIP's research. The EIP's rapid-response research and analysis work necessitated an adaptive, rapid-response communications strategy in order to share timely insights and key mis- and disinformation concepts with journalists and news outlets. One goal was to ensure that misleading narratives were appropriately contextualized in terms of their reach and velocity, to avoid unnecessarily amplifying something false but very sparse. Investigating and reporting on mis- and disinformation is complex and comes with unique challenges.[19] The EIP held regular news briefings in which analysts and team leads prioritized describing and contextualizing the misinformation incidents

documented in tickets. Journalists who attended the briefings could then reach, educate, and inform the communities they served, contextualizing and countering misleading narratives as they saw fit. Over the time of the EIP's operation, this process resulted in over 60 articles that specifically cited the EIP's work or its researchers.[20]

A thoughtful media strategy was key to our reach and impact as an organization. We met the needs of media stakeholders in three primary ways—public research briefings, responding to media requests, and in-depth collaborations.

Public Research Briefings

On October 13, 2020, the EIP hosted the first in a series of weekly research briefings designed to share the Partnership's rapid-response research and policy analysis more broadly ahead of Election Day. Before each briefing, the EIP used its Twitter account, @2020Partnership, to announce the briefing and promote attendance. These briefings, scheduled for 30 minutes, were hosted virtually on Zoom and featured short presentations from various EIP researchers and analysts. Each briefing reserved time for members of news organizations to ask questions of researchers involved with the Partnership. The briefings were considered "on the record," meaning that anything shared or said during the course of the presentations or from the question-and-answer session could be used and directly quoted from by journalists for their reporting. The Q&A format allowed EIP researchers and analysts to cover a lot of ground in a relatively short amount of time while also allowing journalists to gain additional insights from the other questions asked by reporters from other news organizations. As interest in the EIP's work grew and reports of false and misleading information increased dramatically in the days leading up to the election, briefings increased from once a week to several times a week.

The briefings were open to the public. The first briefing hosted approximately 12 journalists, but as interest grew, so did briefing attendance, with an average of 120 attendees on election week briefings and a peak of 174 attendees at the briefing the day after the election. After each briefing, the EIP communications lead followed up with journalists in attendance.

On Election Day, the EIP hosted a morning and afternoon briefing to report on observations of activity that day. Reporters and editors from outlets including the *Washington Post*, the *New York Times*, the *Wall Street Journal*, *USA Today*, *MIT Tech Review*, *Bloomberg Business*, the Associated Press, Reuters, National Public Radio, *Politico*, NBC News, The Markup, The Information, PBS NewsHour, BBC News, Agence France Presse, the *Telegraph*, and Cyberscoop regularly attended.

Responding to Media Requests

Throughout the course of the EIP's work ahead of and after Election Day, our communications lead also fielded inbound requests from the press to assist in assessing specific developing stories. Some of these journalists were dedicated to the "misinformation beat," while others covered peripheral beats such as the election, politics, technology, etc.

The UW team took the lead in tracking and responding to media requests that came in across the Partnership and connecting with the appropriate EIP researcher. For instance, journalists interested in misinformation-related policies developed by social media companies were directed to Stanford Internet Observatory, which closely monitored and analyzed guidelines put forward by platforms. Similarly, journalists interested in EIP research about "repeat spreaders" on Twitter who regularly shared false claims or misleading information about voting procedures were connected with members of the UW team, who were tracking and analyzing how that type of misinformation was shared and amplified.

In-Depth Collaborations

In the days leading up to the election, the EIP set up collaborations with a few journalists who had experience covering the "misinformation beat." These differed from media requests in the length of engagement; in these cases, we set up Slack channels and Google documents to think through trends and emerging data with the journalists, who were also experts in online misinformation. For instance, the UW team fielded more specialized research requests from NBC News, which has dedicated numerous newsroom resources to reporting on mis- and disinformation issues. NBC's Brandy Zadrozny did some of the most substantive reporting on election-related mis- and disinformation ahead of and after Election Day, bolstered by some of the EIP's specialized research. Her election week story about election fraud narratives was driven by this in-depth collaboration.[21] Sheera Frenkel of the *New York Times* spent Election Day co-located with EIP researchers from the Stanford Internet Observatory, with COVID-19 precautions in place. She published an early piece about the emerging "Stop the Steal" narrative, with quotations from an SIO researcher.[22]

The EIP also spent time assisting a local journalist writing specifically about election misinformation in Michigan for the *Detroit Free Press*, whose reporting was funded through a short-term grant from the American Press Institute. The reporter, Ashley Nerbovig, attended numerous research briefings ahead of Election Day and was interested in the EIP's "What to Expect" report that outlined the types of disinformation and misinformation that researchers anticipated would emerge and take root before, during, and after Election Day.[23] A November 17, 2020, article in the *Detroit Free Press* looked at how many of the

EIP's pre-election predictions around voting-specific misinformation emerged in Michigan, where incorrect claims and distorted narratives ran rampant in the days and weeks that followed voting.[24] That *Detroit Free Press* article, featuring interviews with EIP researchers, was republished by *USA Today*[25] and other news publications in the USA Today Network, including the *Arizona Republic*. Although many national newsrooms have one or multiple journalists focused on misinformation, Nerbovig was among the few regional reporters dedicated to covering misinformation from a local perspective, which encouraged us to make researchers available to her as she developed her story.

The EIP's outreach efforts with journalists and media organizations were valuable because they enabled timely sharing of insights and in-depth analysis with the public, policymakers, and social media platforms. During uncertain times, many people turn to journalists. At the same time, journalists themselves were seeking sound information to better contextualize the dynamics of how mis- and disinformation are shared and amplified. By connecting journalists to our research through these media efforts, the EIP was able to have a quick and widespread impact.

Platforms

The EIP established relationships with social media platforms to facilitate flagging of incidents for evaluation when content or behavior appeared to violate platform policies (discussed further in Chapter 6). The EIP reached out to a wide set of social media platforms to engage with the project, and onboarded those that expressed interest in participating. At the start of the EIP analysis period, representatives from the onboarded platforms were granted access to the workspace management system. Analysts conducted their initial assessment on all tickets, and, if content in a ticket appeared to be a violation of a platform's published content policies,[26] an analyst or manager added the platform representative to the ticket. If questions arose, a manager communicated with the platform representative in the ticket comments. Analysts put the ticket back in the queue and updated the ticket to note if the content in question received a moderation action. If analysts identified the content on a ticket as in scope, but not in violation of a platform's published policies, the platform was not tagged.

The EIP onboarded the following social media companies: Facebook and Instagram, Google and YouTube, Twitter, TikTok, Reddit, Nextdoor, Discord, and Pinterest. These platforms were chosen based on several factors including the size of the platform itself, as well as the practical research constraints around the ability to monitor public content on the platform. A platform such as Snapchat, for example, has a large userbase; however, due to its ephemeral content, we did not include this platform in our work.

There were additionally several “alt-platforms” that had no moderation policies, sometimes deliberately so. This included platforms such as Parler, Gab, 4chan, and a handful of message boards. EIP observed false and misleading content on these platforms, but had no interactions with any of their representatives.

1.5 Example Ticket Process

To illustrate the scope of collaboration types discussed above, the following case study documents the value derived from the multistakeholder model that the EIP facilitated. On October 13, 2020, a civil society partner submitted a tip via their submission portal about well-intentioned but misleading information in a Facebook post. The post contained a screenshot (See Figure 1.4).

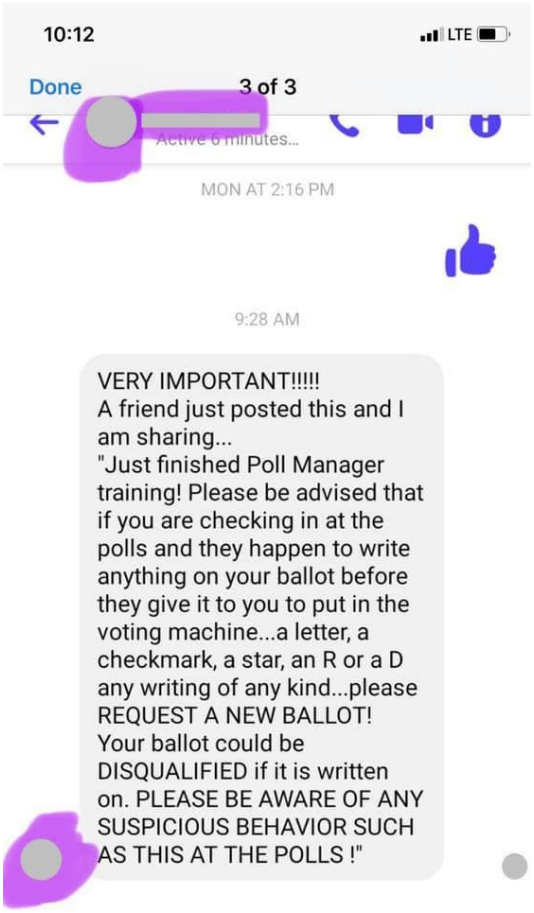

Figure 1.4: Image included in a tip from a civil society partner.

In their comments, the partner stated, “In some states, a mark is intended to denote a follow-up: this advice does not apply to every locality, and may

confuse people. A local board of elections has responded, but the meme is being copy/pasted all over Facebook from various sources." A Tier 1 analyst investigated the report, answering a set of standardized research questions, archiving the content, and appending their findings to the ticket. The analyst identified that the text content of the message had been copied and pasted verbatim by other users and on other platforms. The Tier 1 analyst routed the ticket to Tier 2, where the advanced analyst tagged the platform partners Facebook and Twitter, so that these teams were aware of the content and could independently evaluate the post against their policies. Recognizing the potential for this narrative to spread to multiple jurisdictions, the manager added in the CIS partner as well to provide visibility on this growing narrative and share the information on spread with their election official partners. The manager then routed the ticket to ongoing monitoring. A Tier 1 analyst tracked the ticket until all platform partners had responded, and then closed the ticket as resolved.

1.6 Practical Lessons Learned

The EIP was a first-of-its-kind collaboration between multiple stakeholder types who shared the goal of understanding, and being positioned to rapidly and effectively counter, election-related misinformation. There were several key lessons learned that may be helpful toward informing similar efforts in the future:

Pre-Election Period

1. **Detailed enumeration and comparison of platform policies led to tangible positive changes.** When the EIP was formed in the summer of 2020, no comprehensive comparison of policies around election-related misinformation, or civic integrity, had been published. One of the first efforts of the Partnership was to collect these policies and compare them side-by-side. That policy comparison improved the EIP's quality of content analysis and reporting.

2. **Pre-bunking helped journalists contextualize what they were seeing.** On October 26 the EIP published a blog post predicting the manner and focus of misinformation that its analysts and researchers believed were likely to pervade social media on Election Day and shortly after.[27] This piece was informed by experience from past elections, and observations accrued during the months of monitoring and analysis. Most of the predictions turned out to be accurate. This post, and the subsequent targeted stakeholders briefings around it, provided a rare opportunity to "pre-bunk" narratives

before they reached the mainstream. This sort of effort may be useful in effectively mitigating the effects of misinformation in the future.[28]

3. **Using per-content tickets to represent incidents presented challenges for tracking larger narratives.** As noted in this chapter, the EIP often started analysis by examining content on a very granular level—a ticket might initially represent a single social media post. On the positive side, this approach allowed for nimble Tier 1 analysis, and the Jira platform allowed for aggregation as needed. On the negative side, this approach made tracking narratives significantly more difficult, especially those dormant for a period of time before resurfacing in many online locations at once. Narratives usually spanned multiple types of content pieces across multiple platforms over a broad period of time. While the EIP analysts would eventually merge or link tickets into a broader narrative ticket, this process was labor intensive, and ran the risk of content data getting lost in the effort.

Election Day and Afterward

1. **Public briefings and one-on-one media engagement bolstered real-time information exchange, and helped educate and inform the public.** The EIP's media briefings were not originally a planned part of the effort. However, we found that they were of value for enabling journalists to contextualize observed events and trends and communicate them to the larger public.

2. **The cadence and resource demands of rapid analysis increased as the election cycle progressed, leading to challenges in the logistics of EIP research.** The members of the EIP span the mis- and disinformation research community, which has primarily focused on retrospective analysis. In contrast, demands of the EIP publication schedule represented a novel operational challenge for all organizations involved in a few key ways. First, the EIP analysis and a commitment to quick turnaround required drawing conclusions based on rapidly updating information. Second, the EIP's regular public briefings required updating conclusions and predictions in an episodic manner. Third, a COVID-shortened fall academic quarter for Stanford University and University of Washington student analysts made it challenging to synchronize work after the Thanksgiving break.

1.7 Reading This Report

This report—the conclusion to the Election Integrity Partnership's work—summarizes and details the Partnership's findings since its formation on July

26, 2020. Chapter 2 lays out the metrics and statistics from EIP's detection period, which are the foundation of further analysis. Chapter 3 examines the key false and misleading narratives that emerged and evolved over the course of the 2020 election and after, and Chapter 4 looks at the tactics used to spread the narratives across the information ecosystem. We take a broader perspective in Chapter 5, looking at "repeat spreaders"—individuals, organizations, and media entities that repeatedly promoted numerous false and misleading narratives. In Chapter 6, we review social media platforms' election-related policies and discuss how those policies matured over time and were applied. We conclude the report in Chapter 7 by providing policy recommendations, based on the findings of our work, to government entities, media outlets, platforms, and civil society organizations.

Notes

1. (page 1) Michael McFaul, ed., Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Election and Beyond (Stanford, CA: Cyber Policy Center, June 2019), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/stanford_cyber_policy_center-securing_american_elections.pdf

2. (page 1) Herbert Lin, et al., "Increasing the Security of the U.S. Election Infrastructure" in McFaul, Securing American Elections, 17.

3. (page 2) In Wisconsin, for example, federal district court judge William Conley ruled to extend the acceptance date of absentee ballots from November 3 to November 9, citing that "Wisconsin's election system sets [voters] up for failure in light of the near certain impacts of this ongoing pandemic." The judge put his order on hold to give the Wisconsin State Legislature time to appeal. The Circuit court ultimately overruled the lower court ruling and time ran out for the Wisconsin legislature to legislate or appeal an exception to state election law. See Democratic National Committee v. Bostelmann, No. 20-2835 (7th Cir. October 8, 2020); Amy Howe, "Court declines to reinstate COVID-19 accommodations for elections in Wisconsin," SCOTUSblog, October 26, 2020, 11:28 pm, https://www.scotusblog.com/2020/10/court-declines-to-reinstate-covid-19-accommodations-for-elections-in-wisconsin/

4. (page 5) "Announcing the EIP," Election Integrity Partnership, July 27, 2020

5. (page 8) The platforms we evaluated are: Facebook, Instagram, Twitter, YouTube, Pinterest, Nextdoor, TikTok, Snapchat, Parler, Gab, Discord, WhatsApp, Telegram, Reddit, and Twitch. We published our initial evaluation on August 18, 2020, and updates on September 4, September 11, October 14, October 19, October 27, and October 28, 2020. Twitch was added to our list of evaluated platforms during our blog post update on October 27. Each update

reflected changes in platforms' published policies. See "Evaluating Election-Related Platform Speech Policies," Election Integrity Partnership, October 28, 2020, https://www.eipartnership.net/policy-analysis/platform-policies

6. (page 8) The EIP used Jira Service Desk software for the project. The team chose Jira because it supported a large team and allowed the addition of workflows that require both robust customer management capabilities and organizational features to reflect the numerous roles needed to respond to any inbound request. Licenses and technical support were provided under Atlassian's community license program.

7. (page 9) See Appendix A on page 245: Definitions for a detailed definition of both Events and Incidents.

8. (page 9) See Appendix B on page 249 for the Tier 1 and Tier 2 analysis questions.

9. (page 13) Sean Lyngaas, "Sen. Warner calls for a 'whole-of-society' U.S. cyber doctrine," CyberScoop, December 7, 2018, https://www.cyberscoop.com/sen-warner-calls-whole-society-u-s-cyber-doctrine/

10. (page 14) Common Cause, https://www.commoncause.org/our-work/voting-and-elections/

11. (page 14) NAACP, https://naacp.org

12. (page 14) Stanford-MIT Healthy Elections Project, https://healthyelections.org/

13. (page 14) Defending Digital Democracy Project, https://www.belfercenter.org/project/defending-digital-democracy

14. (page 14) MITRE, https://www.mitre.org

15. (page 14) AARP, https://www.aarp.org

16. (page 14) National Conference on Citizenship, https://ncoc.org

17. (page 14) Elliot Trotter, "CIP, AARP Washington Factcheck Ambassador Trainings help retirees sort fact from fiction," University of Washington Center for an Informed Public, December 16, 2020, https://www.cip.uw.edu/2020/12/16/cip-aarp-washington-factcheck-ambassador-trainings/

18. (page 14) "About Junkipedia," https://www.junkipedia.org/about

19. (page 14) Melinda McClure Haughy, et al., "On the Misinformation Beat: Understanding the Work of Investigative Journalists Reporting on Problematic Information Online," Proceedings of the ACM on Human-Computer Interaction no. 4, Article 133 (October 2020), https://doi.org/10.1145/3415204

20. (page 15) See Appendix E on page 257 for a list of media citations.

21. (page 16) Brandy Zadrozny, "Misinformation by a thousand cuts: Varied rigged election claims circulate," NBC News online, November 11, 2020, https://www.nbcnews.com/tech/tech-news/misinformation-thousand-cuts-varied-rigged-election-claims-circulate-n1247476

22. (page 16) Sheera Frenkel, "The Rise and Fall of the 'Stop the Steal' Facebook Group," *New York Times*, November 5, 2020, https://www.nytimes.com/2020/11/05/technology/stop-the-steal-facebook-group.html

23. (page 16) Kate Starbird, et al., "Uncertainty and Misinformation: What to Expect on Election Night and Days After," Election Integrity Partnership, October 26, 2020, https://www.eipartnership.net/news/what-to-expect

24. (page 17) Ashley Nerbovig, "'Not a whole lot of innovation': 2020 election misinformation was quite predictable, experts say," The Detroit Free Press, November 17, 2020, https://www.freep.com/story/news/politics/elections/2020/11/17/2020-presidential-election-misinformation-predictable-experts/6322926002/

25. (page 17) Ashley Nerbovig, "'Not a whole lot of innovation': 2020 election misinformation was quite predictable, experts say." USA Today, November 17, 2020, https://www.usatoday.com/story/news/politics/elections/2020/11/17/2020-presidential-election-misinformation-predictable-experts/6322926002/

26. (page 17) "Evaluating Election-Related Platform Speech Policies," Election Integrity Partnership.

27. (page 19) Kate Starbird, et al., "Uncertainty and Misinformation: What to Expect on Election Night and Days After," Election Integrity Partnership, October 26, 2020, https://www.eipartnership.net/news/what-to-expect

28. (page 20) Brian Freidberg, et al., "A Blueprint for Documenting and Debunking Misinformation Campaigns," Nieman Reports (October 20, 2020), https://niemanreports.org/articles/a-blueprint-for-documenting-and-debunking-misinformation-campaigns/

Chapter 2

Data and Summary Statistics

2.1 Introduction

The Election Integrity Partnership collected data between September 3, 2020 and November 19, 2020. The dataset we discuss in this part of our report comes from tickets: the internal reports within the EIP's system, each of which identified a unique information event.

Key findings

- We processed 639 in-scope tickets. 72% of these tickets were related to delegitimizing the election results.
- Twitter, Google, Facebook, and TikTok all had a 75% or higher response rate (on the EIP Jira ticketing platform) to tickets they were tagged in.
- Our process got tighter—both within the EIP and in terms of our relationship with the platforms—over time, with the time between ticket creation and platform response dropping substantially as we approached Election Day.
- 35% of the URLs we shared with Facebook, Instagram, Twitter, TikTok, and YouTube were either labeled, removed, or soft blocked. Platforms were most likely to take action on content that involved premature claims of victory.

Tickets

Most tickets created through the EIP's work represent a unique piece of misinformation or disinformation related to election processes. For example, one

ticket was for a Google ad incorrectly claiming that a Florida official had been caught perpetrating a voter fraud scheme. Other tickets discussed a misinformation narrative that appeared across several platforms. Some tickets would focused on a single website that was generating a lot of misinformation. Other tickets discussed incitement to violence—for example, one ticket discussed all cross-platform instances of a single meme instructing people on how to disguise themselves ostensibly ahead of a violent rally. Tickets were primarily created by members of the four core EIP organizations, though 16% of tickets were filed by the Center for Internet Security (CIS), an election official community partner, in the form of tips.

Figure 2.1 on the facing page shows an excerpt of an example ticket. This ticket was created for #Sharpiegate, the narrative that voters were forced to complete their ballots with Sharpie markers that would invalidate ballots. The "Shared with" list shows the organizations tagged on this ticket—tagging an organization is the equivalent of sharing, making the ticket visible to them. The URLs field includes URLs containing or involved in the spread of the misinformation. We discuss the dataset composed exclusively of those URLs in this section of the report as well.

The ticket also has fields for analyst discussion, data that we also extracted and coded. Figure 2.2 on page 30 shows the discussion for the #Sharpiegate ticket. This example shows responses from our government partners, who provided helpful information, and platform responses.

The ticket-level dataset necessarily reflects the biases of those with the authority to create tickets: internal EIP members and external partners. For example, researchers within the Partnership signed up to monitor particular topic groups, such as influencer accounts or Spanish-language content (see Chapter 1, Section 1.3 on page 10 for a list of these groups). Our finite staff and time meant that we prioritized monitoring some content over others; for example, our prioritization of swing states over non-swing states may cause the dataset to understate the amount of misinformation in the latter. Similarly, we were not able to monitor misinformation in languages not widely spoken in America, and as a result our dataset likely understates the amount of foreign language misinformation. While the dataset has these weaknesses, given our large team and cross-platform monitoring, we believe this dataset is important and unique, and that it can shed light on key misinformation narratives and tactics around the election.

In total, the dataset included 639 distinct, in-scope tickets. Following the elections, we coded the tickets to assess what category of election-related misinformation they fell under (for example, participation interference or fraud), what tactics were used (for example, livestream video), what actor was targeted (for example, poll workers or USPS), what state(s) were targeted, and what part of the

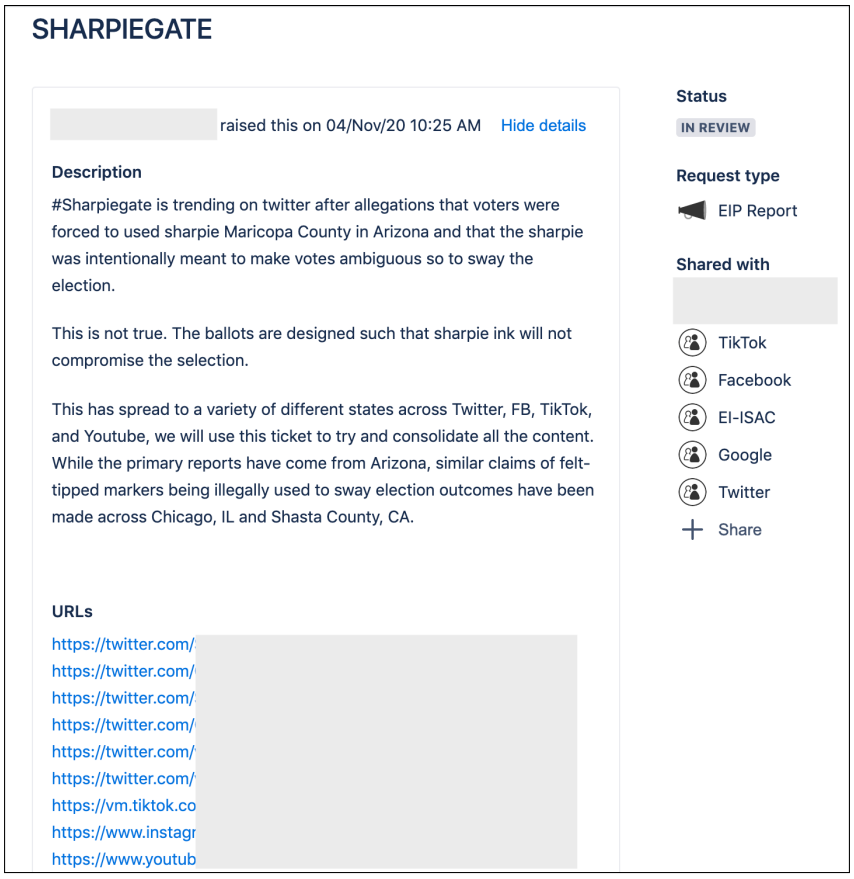

Figure 2.1: An example ticket. We have omitted specific URL information.

electoral process was discussed (for example, voting by mail). Two members of the EIP coded each ticket, and a different member reconciled any discrepancies in coding.

The taxonomy, featuring 10 questions and a total of 71 choices, performed suitably. Intercoder agreement was evaluated with Cohen's Kappa, a metric used to judge coder agreement with consideration for random entries by coders.[1] Cohen's Kappa (K) is represented as a range from 0 to 1, where $K = 0$ indicates random agreement, and $K = 1$ indicates total agreement between coders. Our coding processes and dataset scored $K = 0.629$, which indicates substantial agreement and inspires confidence in the final dataset given the thorough reconciliation process that each ticket went through after its initial coding. The mean percentage agreement across the set was 89.48% with a standard deviation of 0.08%. Given high percentage agreement and a reasonably confident Kappa score, the codified tickets can be reliably used to evaluate our monitoring efforts. We provide more details on findings from the inter-coder reliability analysis in

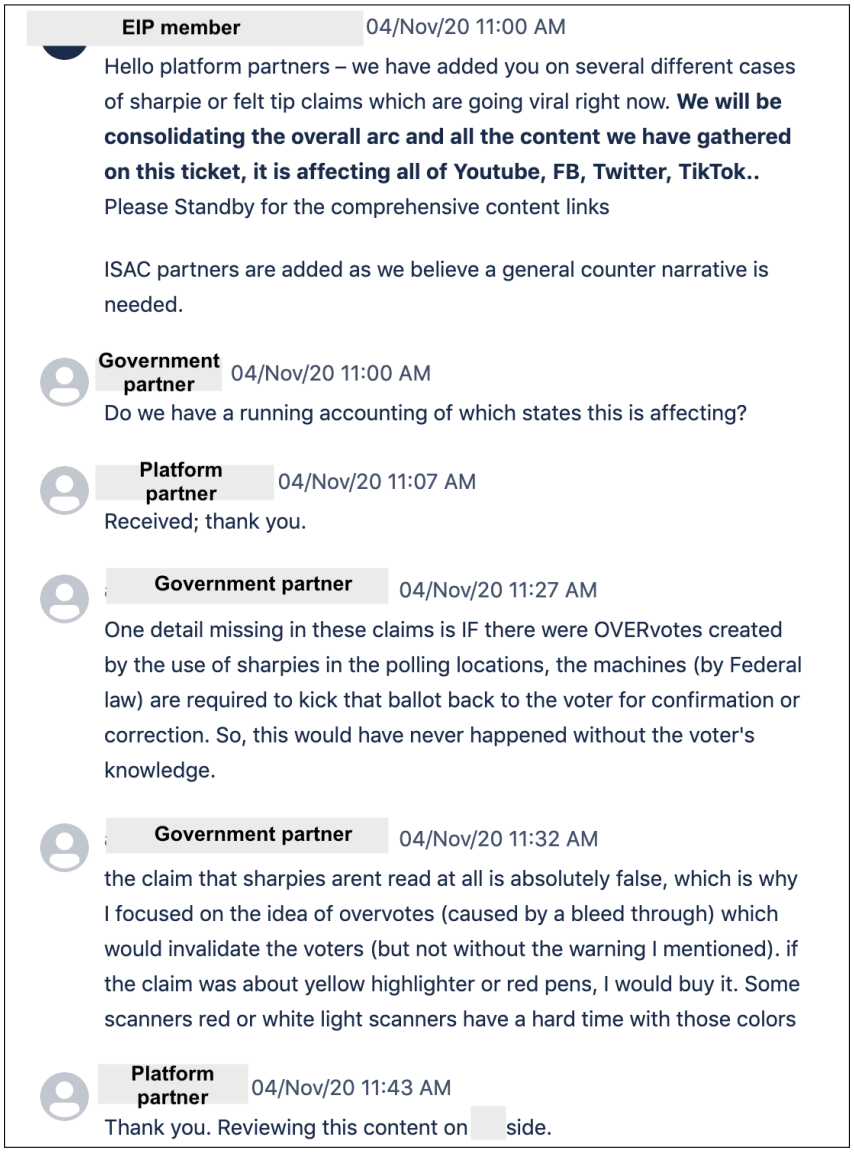

Figure 2.2: Discussion on the #Sharpiegate ticket. The commenters include members of the EIP, government partners, and platform partners.

Appendix B on page 249.

For one of the questions that had lower than normal intercoder agreement—whether or not the ticket related to fraud—we developed a clearer definition of fraud and re-did the coding for all tickets.

Throughout this chapter we will note some important limitations in the dataset. For example, when we discuss platform response rates, these are response rates only from platforms we partnered with. There will be no data for Parler response rates, for example, because Parler was not an external partner of the EIP.

2.2 Summary Statistics

Overview of Tickets

In this section we present summary statistics from the dataset. Figure 2.3 on the following page shows the number of tickets over time, by ticket category. We processed 142 tickets on Election Day, 22% of all tickets. The Election Day spike is likely due to a combination of an increase in election-related online conversations on November 3, significantly more EIP staffing on this day than previous days, and what may have been our partners' greater focus on reporting misinformation on Election Day.

Out of the 639 tickets, 72% were categorized as delegitimization (content aiming to delegitimize election results on the basis of false or misleading claims), 21% as procedural interference (misinformation related to actual election procedures), and 15% as participation interference (posts that include intimidation to personal safety or deterrence to participation in the election process). We note that not all tickets are created equal. Some tickets discussed misinformation that spread far, while other tickets discussed misinformation that might not have been seen by many.

While Chapter 3 will discuss the reach of specific narratives, Table 2.1 on the next page shows the relationship between ticket category and a rough measure of reach that we estimated during the coding process. It suggests that most categories of tickets had a similar distribution of reach, with the exception of fraud narratives, which did not go as widely viral. However, we note that only five of the tickets are categorized as fraud.

Segmentation of Misinformation by Platform and Region

After our last ticket was filed, we coded tickets to assess whether the narrative appeared on one of the platforms we were tracking; of course, many narratives appeared on multiple platforms. 77% of tickets appeared on Twitter, 46% on

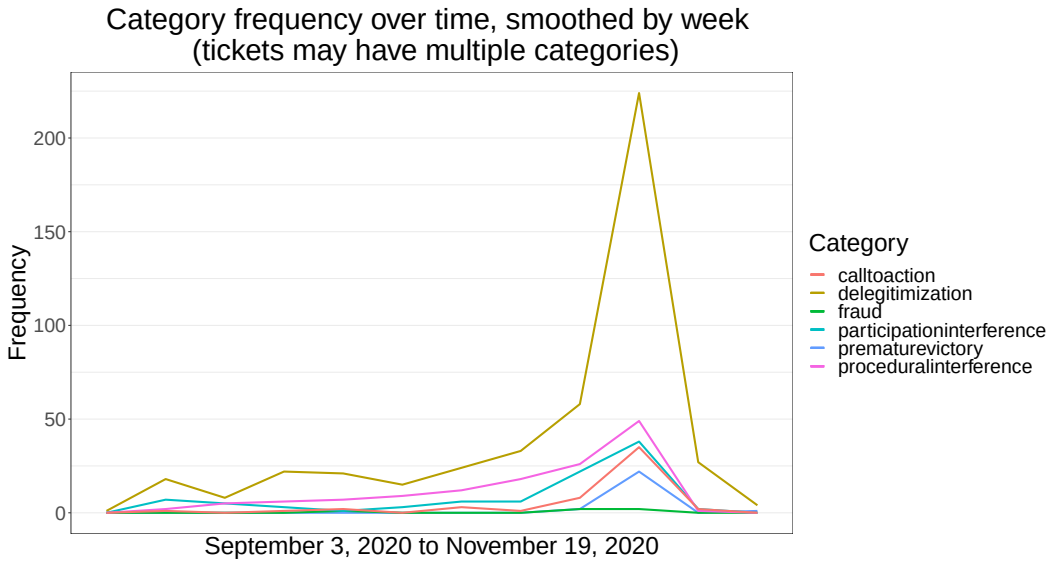

Figure 2.3: Ticket category over time. Tickets may have multiple categories.

	High: >100k engagements	**Medium: 1k–100k engagements**	**Low: < 1k engagements**	**N/A**
Participation Interference	16%	40%	43%	1%
Call to Action	11%	42%	43%	4%
Premature Victory	12%	52%	36%	0
Delegitimiza-tion	15%	49%	35%	1%
Procedural Interference	11%	36%	50%	3%
Fraud	0%	20%	60%	20%

Table 2.1: Relationship between ticket category and estimated reach.

Facebook, 13% on Reddit, 12% on Instagram, 12% on YouTube, and 8% on TikTok. Other platforms, including Parler, 4chan, and Telegram, appeared in less than 5% of tickets. While it is useful to know that the tickets we handled were primarily on the two large platforms—Twitter and Facebook—we caution that these numbers should not be interpreted as "most misinformation appeared on Twitter." Facebook, Twitter, Reddit, and Instagram have reasonably accessible APIs that made it easier for our team to find misinformation on their platforms. The low percent of tickets for Parler, which is not as easy to observe, should not necessarily be interpreted as Parler having less misinformation.

Many of the tickets discussed misinformation that appeared on websites distinct from social media platforms, such as forums and blogs. The top misinformation-spreading websites in our dataset were the far-right forum thedonald.win, moved from the banned subreddit "r/The_Donald," and thegatewaypundit[.]com, a far-right news website. 65% of these tickets involved an exaggeration of the impact of an issue within the election process.

We also coded tickets based on whether they targeted particular states (Figure 2.4 on the following page). 16% of tickets targeted Pennsylvania, 9% targeted Michigan, and 7% targeted Washington. Many of our state-specific tickets were reported by CIS, reflecting the fact that CIS forwarded reports by state and local election officials, and that certain states sent in many reports while others sent few or none.

Tickets by Tactics and Targets

We also coded tickets based on what tactics we observed being used:

- 49% of tickets involved an exaggerated issue.
- 26% of tickets involved an electoral process issue incorrectly framed as partisan.
- 22% of tickets involved misinformation that was shared by verified users.
- 18% of tickets featured content taken out of context from other places or times to create false impressions of an election issue.
- 17% of tickets involved unverifiable claims, such as friend-of-friend narratives.

Figure 2.6 on page 35 shows the portion of tickets containing incidents or narratives that targeted different aspects of the electoral process. Not surprisingly, tickets about voting by mail dominated tickets in September, while tickets about ballot counting spiked during the week of the election.

2. Data and Summary Statistics

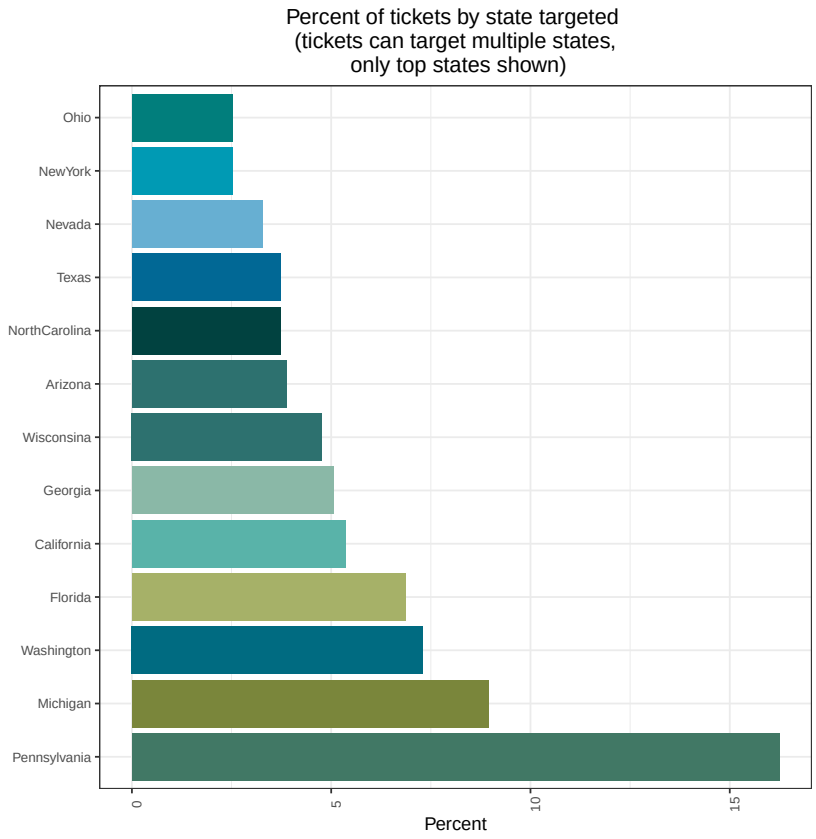

Figure 2.4: Percent of tickets by state targeted.

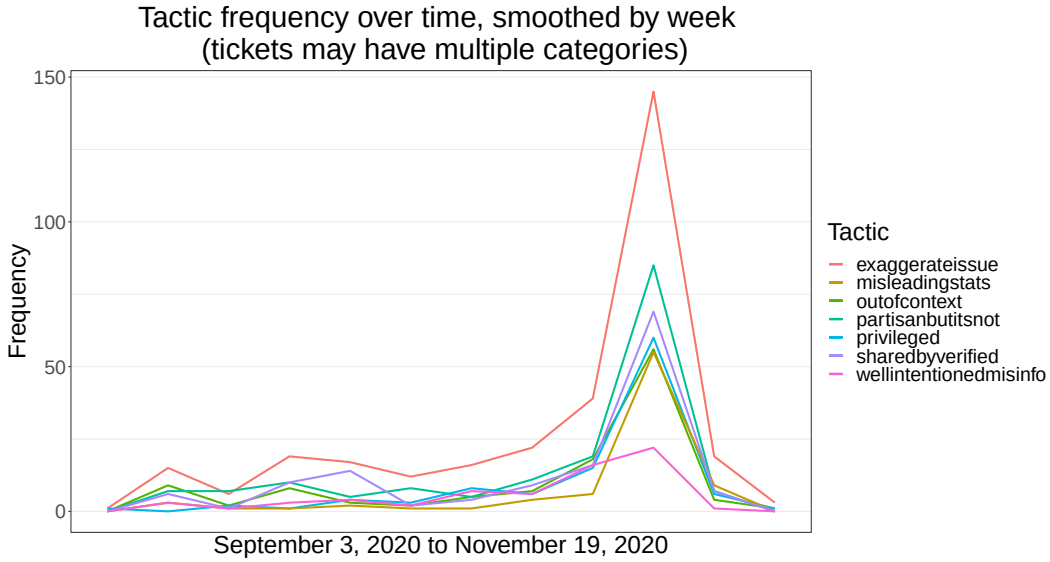

Figure 2.5: Tactic frequency over time.

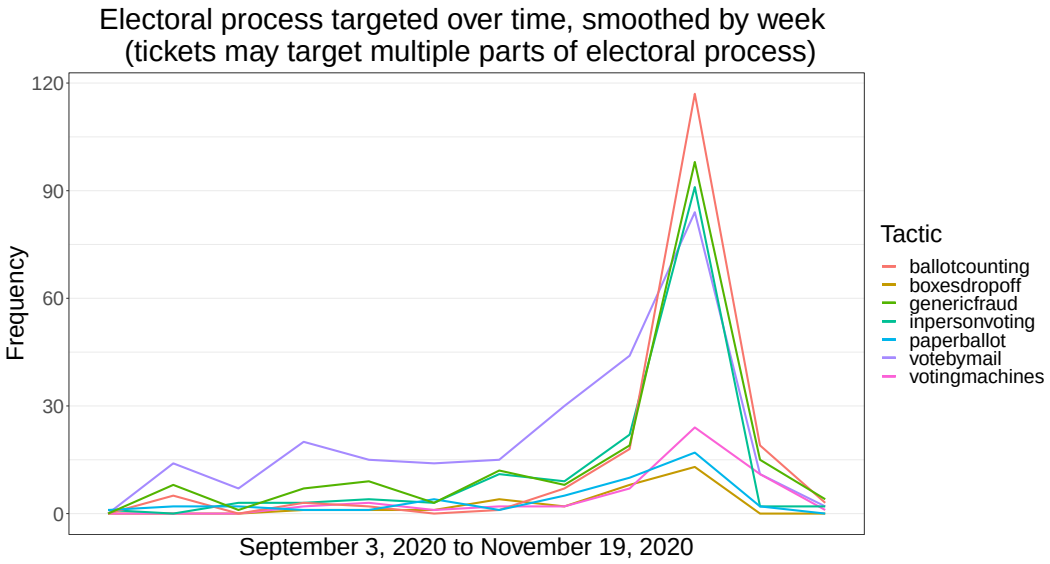

Figure 2.6: Electoral process targeted over time.

Figure 2.7 on the following page shows the actors targeted by the misinformation. The actors most frequently targeted were political affinity groups (for example, Democrats or Republicans, or Biden supporters) with 39% of tickets.

Figure 2.8 on page 37 shows the proportion of tickets that made various claims about the elections. 27% of tickets involved claims about illegal voting.[2]

Last, we coded tickets based on whether they additionally related to COVID-19 narratives, or had an element of foreign interference. Interestingly, just 1% of tickets related to COVID-19, and less than 1% related to foreign interference.

Tickets by Fact-Checking URLs

As the EIP monitored the information space for mis- and disinformation about the 2020 election, analysts consulted published fact-checking resources to assess various claims. 42% of the tickets included fact-checking URLs found by analysts. The most common fact-checking sources were Twitter threads and Facebook posts, often from official government accounts, Snopes, PolitiFact, *USA Today*, the *Washington Post*, and CNN (in that order). The remaining 58% of tickets consisted of misinformation that had low engagement and did not manage to attract the attention of fact-checkers, as well as misleading claims that were not easily falsifiable. Additionally, as noted above, some tickets were about incitement to violence, a topic that does not lend itself to fact-checking. Many tickets included more than one fact-check URL. In total, the dataset included 925 fact-checking URLs.

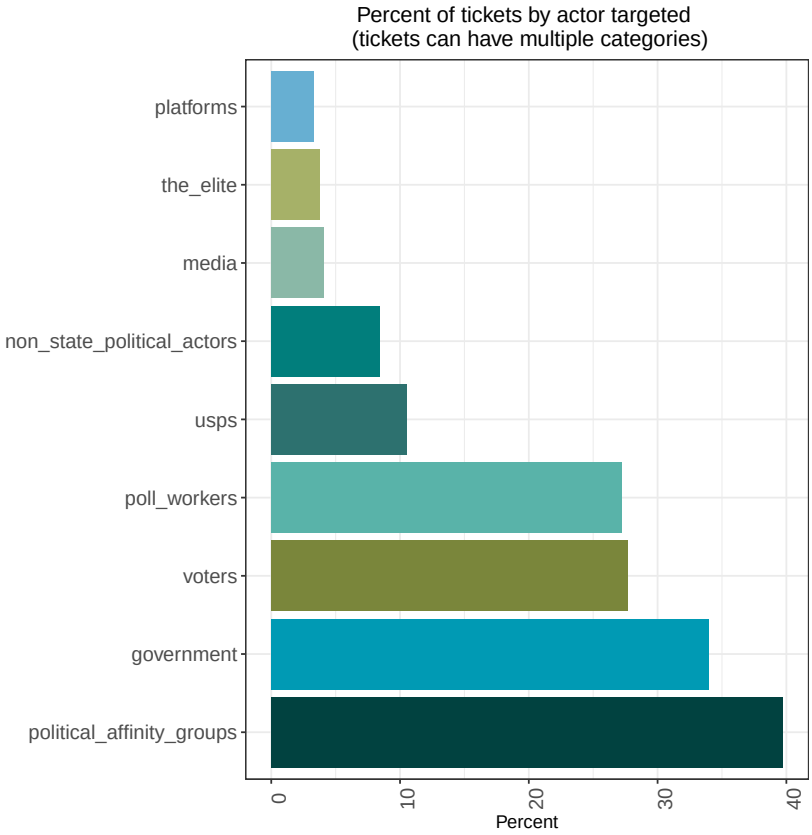

Figure 2.7: Percent of tickets by actor targeted.

Overall, among our tickets we found that higher engagement posts (those with more than 100,000 interactions) contained fact-checking URLs more than posts that had medium to low engagement: 34% of high engagement tickets contained fact-checking URLs, compared to 25% for medium engagement tickets, and 18% for low engagement tickets. EIP researchers also examined the relationship between political ideology and fact-checking, and found that tickets that discussed only left-leaning accounts were as likely to contain fact-checking URLs as tickets discussing only right-leaning accounts.

We also analyzed fact-checking frequency and approaches based on a number of factors, including ticket category. Tickets categorized as "Call to action for protest or mobilization" (often incitements to violence) were least likely to include fact-checking URLs; this makes sense, as these types of tickets are less likely to be appropriate for fact checking.

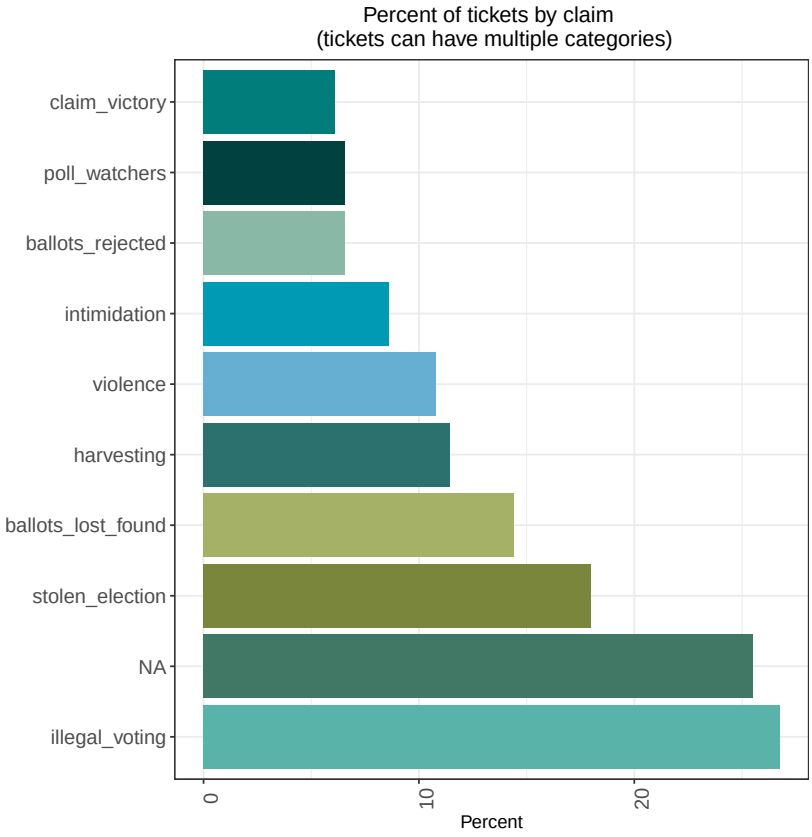

Figure 2.8: Percent of tickets by claim.

2.3 Platform Responsiveness and Moderation Actions Taken

Of our 639 tickets, 363 tickets tagged an external partner organization to either report the content, provide situational awareness, or suggest a possible need for fact-checking or a counter-narrative. Of the tickets in which an external organization was tagged, Figure 2.9 on the following page shows which partner organization was tagged.

In the case where platforms were tagged, we measured the percent of tickets that subsequently received a response from the platforms. A response indicated that the platform confirmed that they were investigating the ticket. We believe these response rates are lower bounds; it is possible platforms investigated tickets, but did not respond on the Jira platform. In total, we believe the four major platforms we worked with all had high response rates to our tickets.

Figure 2.10 on page 39 shows the time between a ticket's creation and the

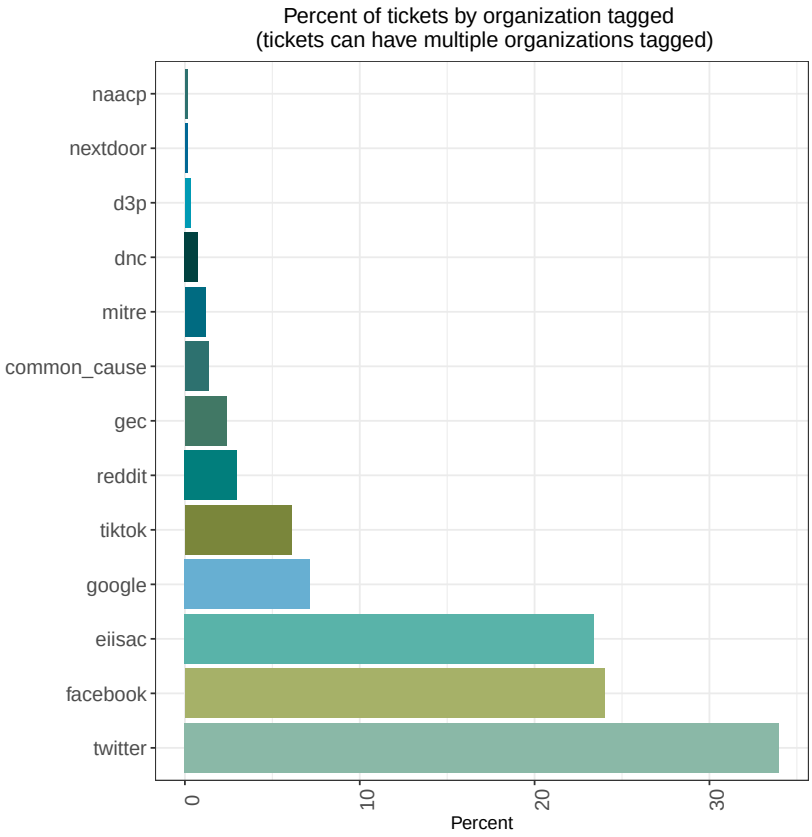

Figure 2.9: Percent of tickets by organization tagged.

	# tickets tagging organization	# tickets that received response	Response Rate
TikTok	40	36	90%
Google	46	41	89%
Twitter	220	185	84%
Facebook	158	120	76%

Table 2.2: Response rate by platform.

platform's response, over time. This data should be interpreted cautiously, as often the ticket creator did not tag the platform; rather, a manager tagged the platform once the ticket was reviewed. So occasionally a ticket was created but the platform not tagged for several hours, or in some rare cases a few days. As such, even if the platforms responded minutes after being tagged, and they often did—particularly on Election Day—this data will not reflect this. However, the data does suggest that the process got much tighter over time. This likely reflects that the EIP shortened the time between ticket creation and platform tagging, and also more engagement from the platforms.

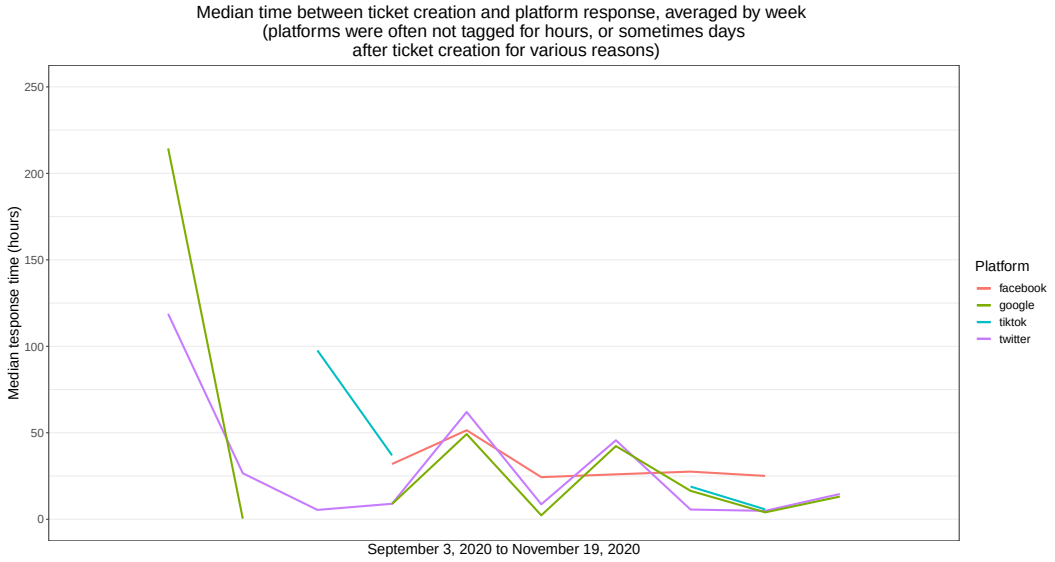

Figure 2.10: Median time between ticket creation and platform response.

Each ticket that tagged a platform partner contained a list of URLs containing the potentially violative content being spread—for example, the URL for a Facebook post or YouTube video. These lists were typically not comprehensive, but intended to highlight a few examples should the platforms decide to investigate further. We developed a web scraping tool that visited each URL to determine what action the platform (limited to Twitter, TikTok, YouTube, Facebook, and Instagram) applied to the content, and ran it on all 4,832 URLs from the tickets on December 7, 2020. The tool evaluated what a US-based individual would see if they visited each URL using the Chrome browser on a desktop computer. For Instagram and Facebook, the visitor was logged in to bypass "login walls." We found no evidence of different users observing different platform actions, so the choice of user did not affect results.

The tool grouped each URL into four possible categories: "removed" when the content was not available (most likely taken down by either the platform or the original poster themselves); "soft block" when the content was only visible by

bypassing a warning (this action was only detected on Twitter); "label" when the platform applied some kind of warning label to the content but did not hide the content; and "none" when the platform took no detectable action. Due to the opaque nature of platforms' ranking algorithms, we were not able to directly detect actions like "downranking." Moreover, because platforms often employ aggressive anti-scraping measures and frequently change their interfaces, it is possible that the scraper incorrectly classified some URLs; in a random sample of several dozen classified URLs, however, we found no errors. In this section we will refer to whether or not platforms actioned URLs, but we note that we cannot distinguish between a platform removing content or a user removing content.

We find, overall, that platforms took action on 35% of URLs that we reported to them. 21% of URLs were labeled, 13% were removed, and 1% were soft blocked. No action was taken on 65%. TikTok had the highest action rate: actioning (in their case, their only action was removing) 64% of URLs that the EIP reported to their team.

Figures 2.11 to 2.14 on pages 40–42 show the distribution of platform action by ticket category, tactic, asset, and claim. Platforms were most likely to take action on tickets that involved premature claims of victory; they took action on these tickets about 45% of the time. They also frequently actioned URLs related to election delegitimization and procedural interference. They were least likely to take action on URLs about fraud, but we note that less than 1% of the URLs had this category. URLs with procedural interference were most likely to be removed.

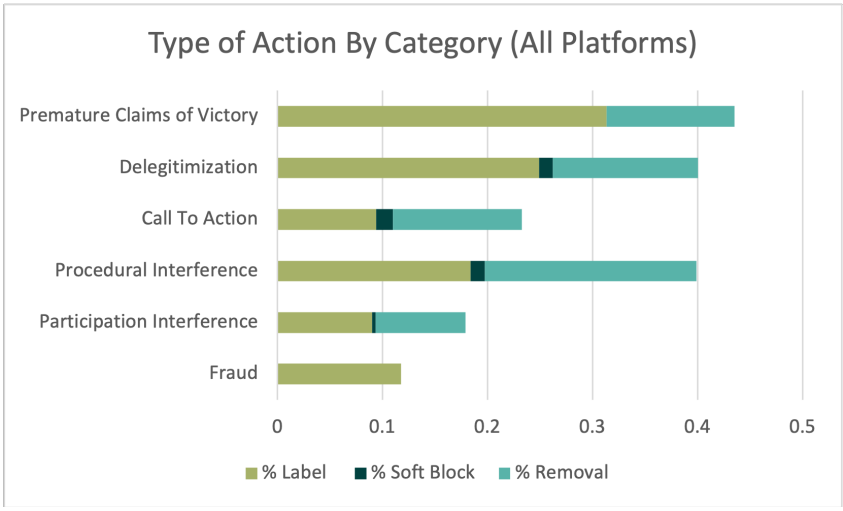

Figure 2.11: Type of action by category.

Platforms were most likely to action URLs that shared misleading statistics, and

most likely to remove phishing content and fake official accounts.

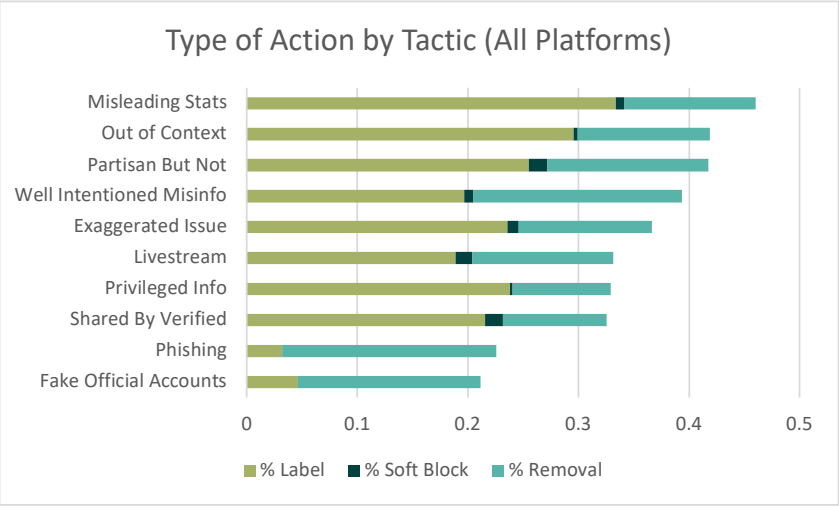

Figure 2.12: Type of action by tactic.

Figure 2.13 shows that there was not large variation in platform action rate across asset types.

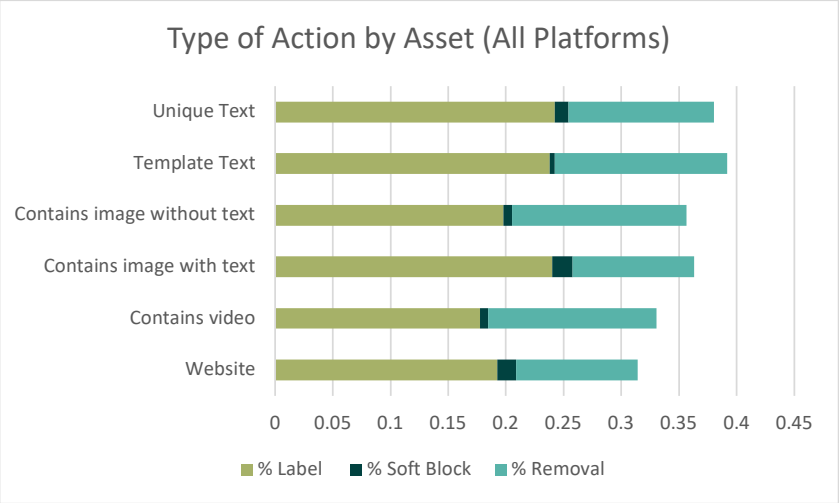

Figure 2.13: Type of action by asset.

More than 50% of URLs that contained premature claims or victory, or claims about the election being stolen, were actioned by platforms. About half of URLs that contained unfounded claims about ballots being rejected were removed—the claim with the highest rate of removal after incitement to violence.

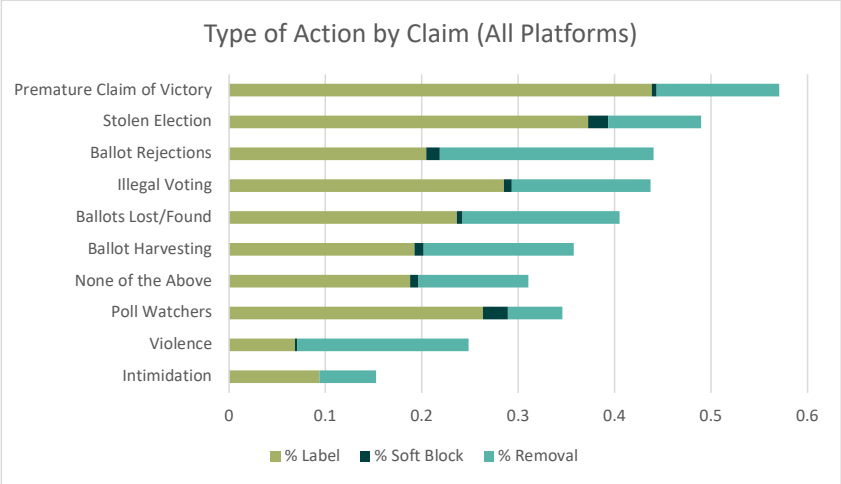

Figure 2.14: Type of action by claim.

2.4 Concerns by Reporting Collaborators

While 79% of tickets were created in-house, CIS reported 16% ($N = 101$) of our tickets. Most reports from CIS originated from election officials. Compared to the dataset as a whole, the CIS tickets were (1) more likely to raise reports about fake official election accounts (CIS raised half of the tickets on this topic), (2) more likely to create tickets about Washington, Connecticut, and Ohio, and (3) more likely to raise reports that were about how to vote and the ballot counting process—CIS raised 42% of the tickets that claimed there were issues about ballots being rejected. CIS also raised four of our nine tickets about phishing. The attacks CIS reported used a combination of mass texts, emails, and spoofed websites to try to obtain personal information about voters, including addresses and Social Security numbers. Three of the four impersonated election official accounts, including one fake Kentucky election website that promoted a narrative that votes had been lost by asking voters to share personal information and anecdotes about why their vote was not counted. Another ticket CIS reported included a phishing email impersonating the Election Assistance Commission (EAC) that was sent to Arizona voters with a link to a spoofed Arizona voting website. There, it asked voters for personal information including their name, birthdate, address, Social Security number, and driver's license number. Other groups that reported tickets include the State Department's Global Engagement Center, MITRE, Common Cause, the DNC, the Defending Digital Democracy Project, and the NAACP.

2.5 Final Observations

This chapter has focused on our ticket-level dataset, which offers a look at the work of the EIP through the duration of our activity. In Chapter 3 of this report we will delve into some of the narratives within the EIP tickets, examining those that achieved the greatest reach or were instrumental for a significant duration of the time leading up to, and following, Election Day.

Notes

1. (page 29) Cohen's Kappa weighs chance in its scoring by evaluating the probability of agreement and the probability of random agreement. The probability of agreement minus the probability of random agreement divided by 1 minus the probability of random agreement is how Kappa is calculated. With this in mind, a Kappa value that is less than zero indicates that there is less agreement than chance and is evidence that the taxonomy or intercoder process is somehow flawed.

2. (page 35) "Political affinity groups" includes references to "the Democrats" or "the Republicans" or particular politicians. "Government" refers to any government entity. "Non-state political actors" includes groups like Black Lives Matter or antifa. "The elite" references people like George Soros or Bill Gates. "Platforms" references social media platforms like Facebook. Voters, poll workers, USPS, and the media are self explanatory.

Chapter 3

Incidents and Narratives: The Evolution of Election Misinformation

3.1 Introduction

The 2020 election was the subject of hundreds of false and misleading claims about voter qualifications, voting processes, and even the basic nature of American democracy. Some claims spread like wildfire across social media only to fade just as quickly. Others circulated unnoticed for days or weeks before igniting with lasting viral momentum. Sometimes, contradictory claims battled for supremacy. Other times, they settled into a surreal coexistence. Some of these claims would ultimately form the foundation of "Stop the Steal"—the 2020 election's most expansive and enduring misinformation narrative, which ultimately culminated in the January 6, 2021, insurrection at the US Capitol—though it was a long and complicated journey.

In this chapter, we examine some of the 2020 election's most noteworthy pieces of election-related misinformation, exploring the character of these claims and charting the messy process by which claims coalesced into broader narratives. We also trace how one narrative gave way to another, forming a conspiratorial canon that is likely to persist for many years to come. In order to identify and differentiate these narratives, we consider the following questions:

What was the first claim that formed the basis of a given narrative? Was there a precipitating event? How did the story develop? What pieces or types of content helped shape it? How did the narrative echo and build upon the narratives that preceded it? How did it bolster the narratives that followed it? Indeed, did it fade away at all?

We begin the chapter with a discussion of our methodology and definitions.

From there, we explore the evolution of narratives in the 2020 election, following their progression to the events of January 6. Then, we discuss the spread of misinformation narratives in non-English communities, focusing on Chinese- and Spanish-speaking Americans (foreign state-backed actors in the 2020 election are described in a box somewhere). Finally, we examine the obstacles these dynamics posed to fact-checkers, and conclude with observations regarding the narrative landscape as a whole.

Because the purpose of democratic elections is a transparent, regularized transfer of political power, they are gravely endangered by misinformation narratives. If citizens are made to feel that a vote was compromised or rigged, then the election cannot be trusted. If the election cannot be trusted, then (at least in the mind of the true believer of such narratives) the democracy itself is invalid. Looking back on the election of 2020 and the January 6 attack, this chapter addresses the resounding question: how did we get here?

3.2 Narratives: Methodology and Identification

Narratives are stories. They draw from a common set of building blocks—characters, scenes, and themes—and assemble them in novel ways. Good narratives inspire suspense and excitement in their audience.[1] A successful book, for instance, is one whose narrative clings to the imagination of its reader. Similarly, a successful conspiracy theory is one whose narrative is especially compelling and emotionally resonant—the audience itself is made to feel that they are the protagonists in a story that only they can interpret and understand.

In daily life, the creation of narratives is aided by a parallel process of framing. Frames are mental schemas that shape how people interpret the world; they highlight specific pieces of information, as Robert Entman writes, "in such a way as to promote a particular problem definition, causal interpretation, moral evaluation and/or treatment recommendation for the item described."[2] Framing, i.e., the production of frames, is a process of selecting certain information and providing a kind of scaffolding that shapes how people interpret a series of events. (The process of framing will be explored in greater detail in Chapter 4.)

Viral misinformation works by decontextualizing and recombining real-world events into compelling narratives with minimal regard for the truth. Some of these narratives are "bottom-up," in which a narrative emerges organically from the post hoc interpretation of disparate events and claims, often beginning with a single post by an individual user. Others are "top-down," consciously created and first disseminated by one or more powerful media or social media influencers. Often, the reach and staying power of certain narratives becomes clear only after the precipitating event has concluded. In complex events like

the 2020 election, multiple narratives can exist side by side, contradicting or reinforcing each other and receiving widely variable attention.

The Election Integrity Partnership's initial monitoring for voting-related misinformation focused on claims, not narratives. Each of the 639 tickets in the EIP database was tied to a particular claim: a fake viral video of ballots being burned, for instance, or an allegation that a Philadelphia poll watcher was improperly barred from entering a voting precinct.

The work of narrative identification began on November 30, 2020, after the EIP's monitoring mission had concluded. We first grouped tickets into "information cascades," or incidents, tracing how a single real-world event (like a video of poll workers collecting ballots in California) could generate a number of different false claims, spread at different rates on different platforms by different actors. After that, we grouped similar incidents together, collapsing them into a small number of distinct narratives. In some cases, the narratives coalesced into umbrella meta-narratives. These narratives formed the basis of the information conflict that would consume the 2020 election.

3.3 The Evolution of Narratives in the 2020 Election

The most destructive misinformation narratives came in waves. As fresh events presented themselves and public attention shifted, old narratives lent their momentum and "evidence" to new ones; incidents were framed so as to "prime" audiences to perceive future similar events as part of a broader pattern. This meant that, while specific falsehoods and delusions might fade, they were never truly forgotten. This process carried some Americans from their first exposure to voting-related misinformation in the summer of 2020 all the way through the violent, far-reaching conspiracy theories that compelled them to storm the US Capitol on January 6.

In the lead-up to the 2020 election, misinformation centered on mail-in voting: the destruction and discarding of real ballots and the "discovery" of fake ones. Such misinformation typically took the form of misleading photos or decontextualized video clips of crumpled mail allegedly found in dumpsters or abandoned trucks. This misinformation was widely amplified by Republican politicians and far-right operatives, including by the Trump White House. After the election, public polling indicated a lack of trust in mail-in voting;[3] while it is difficult to state to what extent that was caused by the media and social media activity, given the amount of misinformation about the process spread from the start, this finding is not surprising.

Concurrently, other popular misinformation narratives suggested that the election had been "stolen" before it even took place. Concerns about disproportionate mail-in voting by Democrats and disproportionate in-person voting by Republicans led partisans on both sides to fear that there would be a manipulation of votes on election night. The Trump campaign primed Republican voters to expect wrongdoing by calling for an "Army for Trump" to safeguard the polls. In turn, Democrats worried that polling places might be invaded by far-right militias. And far-right activists argued that the United States was held in the grip of a "color revolution" orchestrated by an imagined "Deep State" intent on stealing the election.

On November 3 and immediately afterward, misinformation shifted to focus on vote counting and tabulation. This was embodied by the #Sharpiegate narrative, which alleged that poll workers were giving felt-tip pens to voters in conservative precincts to render their ballots unreadable. Despite repeated attempts to debunk it, the narrative found a receptive audience who set to work flooding all social platforms, mainstream and niche, with the claim. After #Sharpiegate gained viral traction, it drew hundreds of Trump supporters to protest outside the recorder's office of Arizona's Maricopa County.

As millions of mail-in ballots were slowly counted and voting returns shifted to favor Joe Biden, this anger and disbelief intensified. A growing swell of misinformation narratives, including Sharpiegate, coalesced under the hashtag #StopTheSteal, which spawned a movement of the same name. Some narratives claimed that hundreds of thousands of deceased citizens had cast Democratic votes; others suggested that Trump was one lawsuit away from victory. Together, these narratives infused their followers with a sense of urgency and a call to action.

As Stop the Steal grew in popularity over the next two months, its allegations of legal and procedural fraud were supplemented by increasingly colorful, outlandish conspiracy theories. Some claimed that Trump's loss had been the work of a CIA supercomputer commissioned by former President Barack Obama. Others argued that Trump's loss had been orchestrated by Dominion Voting Systems, a company that was (falsely) tied to Bill Gates, George Soros, or even the government of Venezuela. The more that these narratives took hold, the further their believers slipped from reality.

Throughout the entire voting period, both Democrats and Republicans had been consumed by fears of election-related violence—of the Proud Boys targeting Black Lives Matter protesters or secret "antifa comrades" infiltrating conservative polling locations. Outside of a surge in use of the #civilwar hashtag on

Twitter, however, little of this rhetoric translated into action in the immediate aftermath of the election. Instead, the creep toward organized violence occurred more slowly. It would explode with fury on January 6, 2021, changing the course of American politics with it.

Ballot-Related Narratives

Setting the Stage for Ballot Irregularity Claims

The process by which votes were cast in the 2020 election was significantly influenced by the global COVID-19 pandemic. By September, when the EIP began monitoring election-related misinformation, nearly 200,000 Americans had already died from COVID-19.[4] In order to prevent COVID-19 transmission at crowded polling places and to accommodate citizens who preferred not to come to the polls, a number of states opted to expand the qualifications for absentee ballots or to alter the vote-by-mail process. For example, dozens of states significantly increased the use of ballot drop boxes.[5]

Changes to electoral processes and sometimes-unclear communications regarding the changes created an ecosystem ripe for mis- and disinformation around the mechanics of voting. Experts predicted that Democrats would rely on mail-in voting more than Republicans,[6] a reality that resulted in the rapid politicization of the process and that stymied many attempts to make it clearer or more accessible.[7] Meanwhile, legitimate confusion about voting procedures offered political activists, influencers, and politicians a receptive environment to sow doubt in the integrity of the voting process as a whole.

General concerns related to mail-in ballots constituted the most prominent type of misinformation assessed in the months before Election Day (see Figure 3.1 on the next page), foreshadowing claims of mass irregularities and "found ballots" following the election. The EIP processed tickets that included claims of mail dumping; mistreated, shredded, or dumped ballots; non-eligible people casting ballots (e.g., dead voters); ballots cast on behalf of others; and voting multiple times by mail.

In this section we highlight two types of ballot-related narratives: "bottom-up" misinformation rooted in real-world events reported by concerned individuals, and "top-down" mis- and disinformation in the form of claims of hidden conspiracies first made by influencers and media personalities who had political or financial incentive to spread falsehoods (see Figure 3.2 on page 53). For the former, we present some claims related to found, discarded, and destroyed ballots, primarily isolated instances of wrongdoing reframed and misconstrued in partisan terms. For the latter, we discuss a video created by Project Veritas (described below), shared widely by right-wing influencers, that claimed

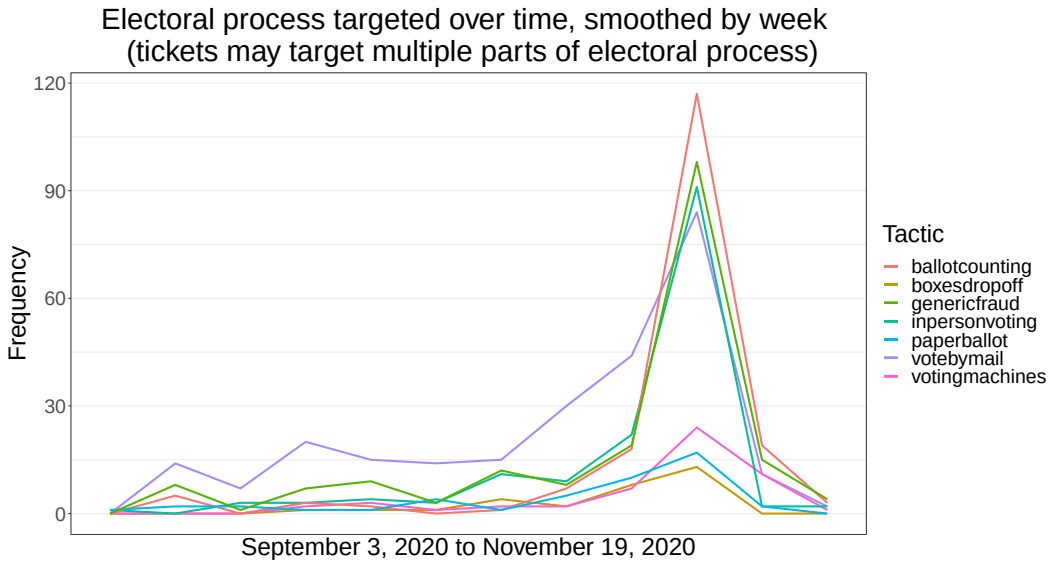

Figure 3.1: The number of tickets that targeted different parts of the electoral process. The spike of tickets occurred on Election Day.

the existence of widespread fraud in the form of ballot harvesting funded and condoned by political elites.

Misinformation For and By the People: How Documented Incidents of Found, Discarded, or Destroyed Ballots Became Narratives

Allegations of mail dumping—real or purported—can be used to mislead audiences in service of particular agendas, such as undermining confidence in mail-in voting or advancing claims that the election is rigged. Narratives around found, discarded, or destroyed ballots circulated through various platforms before, during, and after the election. Though it is illegal for US Postal Service (USPS) letter carriers or related partners to improperly dispose of mail, it does sometimes occur. Overall, however, the USPS is overwhelmingly secure and letter carriers face severe penalties for dumping mail, including jail time.[8]

The incidents in EIP tickets ranged from claims of a handful of ballots found on the side of the road or under a rock to allegations of hundreds of thousands of ballots lost at once in Pennsylvania. Mail-dumping narratives also connected disparate real-world events, pulling them into a broader storyline in which these were falsely portrayed as frequent occurrences, and in which each individual incident was cited as further evidence of an irreparably corrupt and broken system. The EIP team identified five techniques used to leverage these real incidents for broader purposes:[9]

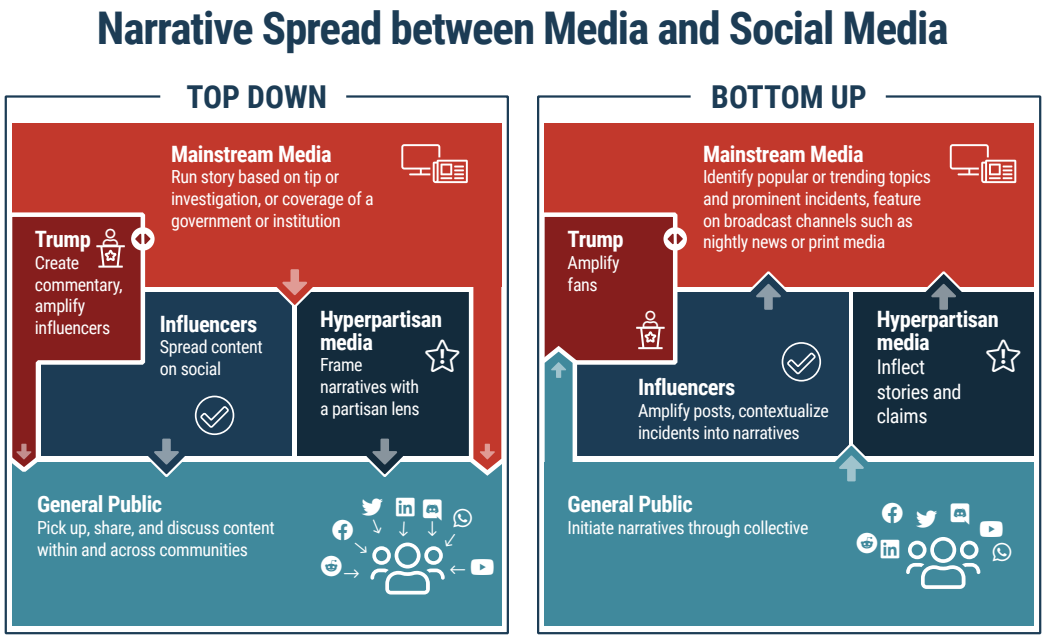

Figure 3.2: Pathways of top-down and bottom-up narratives.

- **Falsely assigning intent:** Acts that are not political are framed as political. For example, a local mail-dumping event is falsely framed as specifically targeting voters on one side of the political spectrum or a mail carrier is identified as "Democratic" or "Republican" to suggest malicious intent. Other times, too much significance is given to the demographics of the locality in which an event occurs. Though these cases may at times contain added falsehoods, often they will rely more on implication than assertion—and are therefore hard to refute with fact-checking.
- **Exaggerating impact:** Real-life incidents are highlighted, selectively edited, or otherwise exaggerated to give a false appearance of substantial impact on election results or to suggest a widespread pattern of misbehavior.
- **Falsely framing the date:** Old events are reframed as new occurrences, such as the recirculation of a 2014 video of a mail carrier dumping mail accompanied by allegations that this was happening in the final weeks of the 2020 election.
- **Altering locale:** Those disseminating the misinformation alter the locale of an event to make it seem more relevant to an audience. For example, photos from a Glendale, California, incident are reframed as having happened in a different local community.

- **Strategic amplification:** In addition to false framing, the usual amplification concerns apply, with the potential for honest or not-so-honest mistakes about intent, actors, times, and locales to be amplified by domestic networks of politically motivated accounts and possibly even foreign actors.

Allegations of deliberately destroyed ballots took various forms, including claims of ballot boxes being lit on fire, mail-in votes being shredded, and foreign actors stealing mailboxes. Occasionally there were legitimate claims, such as accurate reports of attempted arson (one example was in Baldwin Park, California). However, most were easily disproved falsehoods: for example, claims of shredded ballots for President Trump in Pennsylvania in reality were unaddressed applications for mail-in ballots.[10]

The earliest ballot-related story that the EIP collected and analyzed took place within days of launching our monitoring effort in early September. The incident, which occurred in Glendale, California, and involved improperly discarded mail, was incorporated into a broader narrative focused on undermining trust in the USPS and exaggerating the potential impact on the election of this and similar events in California, Wisconsin, and other states. Throughout the election, similar incidents of discarded mail (with and without ballots) were repeatedly framed as fraud, particularly by hyperpartisan online media, and the specific claims of individual stories were amplified and woven into other narratives meant to cast doubt on the integrity of the election.

Glendale, California

In early September, a salon worker in Glendale, California, found multiple bags of unopened mail in a dumpster and took video footage with her cellphone.[11] There is no evidence that any ballots were among the discarded mail; the American Postal Workers Union stated the recovered mail would go through a verification process and be delivered.[12] However, politically motivated actors began using the above techniques of falsely assigning intent, exaggerating impact, and strategic amplification to falsely frame this situation in such a way as to undermine trust in mail-in voting.

The incident was picked up by conservative influencers, including Charlie Kirk and Adam Paul Laxalt. The image below shows a map of popular accounts tweeting about the Glendale mail-dumping incident. The graph reveals an imbalance between left- and right-leaning amplification: the conservative side of the network had more posts than the liberal side and nearly three times as many retweets. Conservative tweets claimed that this mail-dumping incident proved that mail-in voting was not secure because of either incompetence or deliberate sabotage by the USPS and thus should not be allowed. On the liberal

side, influencers promoted a different narrative—that President Trump was deliberately sabotaging the USPS to reduce the number of Democratic votes—and stressed the importance of preserving mail-in voting. As people lost faith in the mail system, some on the left also used the narrative to push people to vote in person or via drop boxes. This bottom-up misinformation, coming first from concerned citizens and then amplified by influencers to, in turn, target average platform users, is a tactic that the EIP would continue to see throughout the election cycle. Overall, the story impacted the perception of the security of voting by mail for both liberals and conservatives.

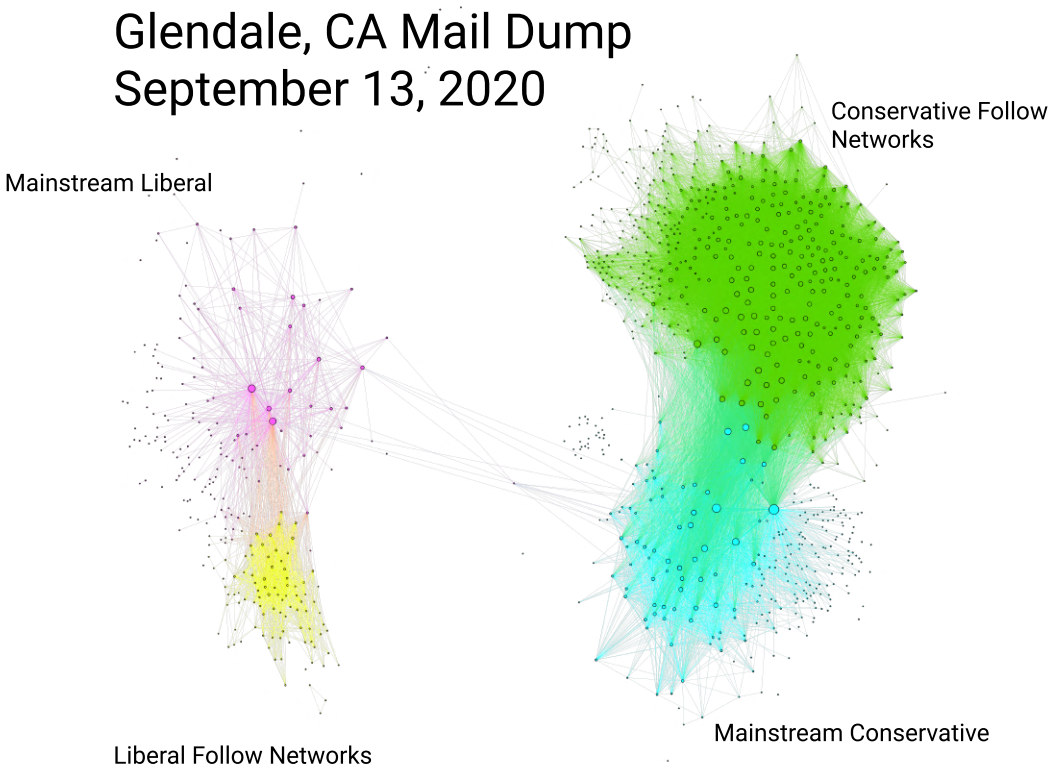

Figure 3.3: The network of influential left- and right-leaning tweets and retweets about the Glendale mail-dumping incident, where the conservative side of the network had nearly three times as many retweets. An animated version of this graph can be found in the EIP's blog post, "Emerging Narratives Around 'Mail Dumping' and Election Integrity."[13]